IN THE SUPREME COURT OF INDIA
[CRIMINAL APPELLATE JURISDICTION]

SPECIAL LEAVE PETITION (CRL.) NO. OF 2014

[Against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014.]

IN THE MATTER OF:

UNIQUE IDENTIFICATION AUTHORITY
OF INDIA & ANR.. ...PETITIONERS

VERSUS

CENTRAL BUREAU OF
INVESTIGATION & ANR. ..RESPONDENT

VOLUME-I

WITH

CRL.MP.NO._____OF 2014

[An application for exemption from filing Certified Copy of Impugned Order and Judgement]

PAPER BOOK

[FOR KINDLY SEE INSIDE]

ADVOCATE FOR THE PETITIONERS: .D.S. MAHRA.

IN THE SUPREME COURT OF INDIA
[CRIMINAL APPELLATE JURISDICTION]

SPECIAL LEAVE PETITION (CRL.) NO. OF 2014

[Against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014.]

IN THE MATTER OF:

UNIQUE IDENTIFICATION AUTHORITY
OF INDIA & ANR.. ...PETITIONERS

VERSUS

CENTRAL BUREAU OF
INVESTIGATION & ANR. ..RESPONDENT

VOLUME-I

WITH

CRL.MP.NO._____OF 2014

[An application for exemption from filing Certified Copy of Impugned Order and Judgement]

PAPER BOOK

[FOR KINDLY SEE INSIDE]

ADVOCATE FOR THE PETITIONERS: D.S. MAHRA.

INDEX

SL. NO.	PARTICULARS	PAGE NOS.
1.	Office Report on Limitation	"A"
2.	Listing Proforma	A1-A3
3.	Synopsis and List of Dates	B–L
4.	Against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014. [Impugned From]	1-7
5.	Special Leave Petition with Affidavit	8-41
6.	**ANNEXURE:P-1** A true copy of the said notification dated 28.01.2009	42-46
7.	**ANNEXURE:P-2** A True copy of the Process Committee minutes which recommended the basic structure of UIDAI dated nil	47-53
8.	**ANNEXURE:P-3** A Copy of the Government of India (Allocation of Business Rules) in exercise of the powers conferred by Clause (3) of Article 77 of the Constitution dated nil.	54-61
9.	**ANNEXURE:P-4** A Copy of the Bio-metrics Standards Committee report dated nil.	62-160

10. **ANNEXURE:P-5**

A copy of the "Demographic Data Standards and Verification Procedure Committee Report" dated nil — 161-196

11. **ANNEXURE:P-6**

Details of these banks arranged in alphabetical order dated nil. — 197-202

12. **ANNEXURE:P-7 (Colly)**

(i). True Copy of the Judgment and order dated 14.9.2011 passed by this Hon'ble Court in W.P.No.196 of 2001 — 203-221

(ii) True Copy of the Judgment and order dated 6.2.2013 passed by this Hon'ble Court in C.A.No.958 of 2013 — 222-238

13. **ANNEXURE:P-8**

A true copy of the Role of Biometric Technology in Aadhaar Enrolment report dated Nil. — 239-269

[Please See Annexure:P-9 to P-19 and application for exemption from filing certified copy of impugned order in Volume No.II]

A

IN THE SUPREME COURT OF INDIA
CIVIL APPELLATE JURISDICTION

SPECIAL LEAVE PETITION (CRL.) NO._____OF 2014

IN THE MATTER OF:

UNIQUE IDENTIFICATION AUTHORITY
OF INDIA & ANR.. ...PETITIONERS

VERSUS

CENTRAL BUREAU OF
INVESTIGATION & ANR. ..RESPONDENT

OFFICE REPORT ON LIMITATION

1. The petition is/are within time.

2. The Petition is barred by time and there is delay of ___days in filing the special leave petition against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014 and petition for condonation of ___days delay has been filed.

3. There is delay of ___days in re-filing the petition and petition for condonation of ___days delay in re-filing has been filed.

BRANCH OFFICER

Dated: .03.2014

A1

PROFORMA FOR FIRST LISTING

SECTION:II

The case pertains to (Please tick/ check the correct box):-

☐	Central Act: (Title)	**Central CR.P.C.**
☐	Section:	**Section 91 of Cr.P.C.**
☐	Central Rule: (Title)	**N.A.**
☐	Rule No(s):	**N.A.**
☐	State Act: (Title)	**N.A.**
☐	Rule No(s):	**N.A.**
☐	Impugned Interim Order: (Date)	**Final 26.02.2014**
☐	High Court: (Name)	**High Court of Judicature at Bombay Bench at Goa**
☐	Names of Judges:	**Hon'ble Smt: R.S.DAlvi and F.M.Reis, JJ**
☐	Tribunal/ Authority: (Name)	**Authority**

1.	Nature of matter:	[ ] Civil	[_/]Criminal
2.(a)	Petitioner/ appellant No. 1:		**Unique Identification Authority of India & Anr.**
(b)	e-mail ID:		**N.A.**
(c)	Mobile phone number:		**N.A.**
3.(a)	Respondent No.1:		**Central Bureau of Investigation & Anr.**
(b)	e-mail ID:		**N.A.**
(c)	Mobile phone number:		**N.A.**
4.(a)	Main category classification:		**14-CRIMINAL MATTERS**
(b)	Sub classification:		**1418-OTHERS**

A2

5.	Not to be listed before:			N.A.	
6.	Similar/Pending matter:			N.A.	
7.	Criminal Matters:				
(a)	Whether accused/convict has surrendered:			[ ]Yes	[ ]No
(b)	FIR No.	N.A.	Date:	N.A.	
(c)	Police Station:			N.A.	
(d)	Sentence Awarded:			N.A.	
(e)	Sentence Undergone:			N.A.	
8:	Land Acquisition Matters:				
(a)	Date of Section 4 notification:			N.A.	
(b)	Date of Section 6 notification:			N.A.	
(c)	Date of Section 17 notification:			N.A.	
9.	Tax Matters: State the tax effect:			N.A.	
10.	Special Category (first petitioner/appellant only):				
	(i) [X] Senior citizen > 65 years			(ii) [X] SC/ST	
	(iii) [X] Woman/child			(iv) [X] Disabled	
	(v) [X] Legal Aid case			(vi) [X] In custody	
11.	Vehicle Number (in case of Motor Accident Claim matters):			N.A.	
12.	Decided cases with citation:			N.A.	

Date: 13.3.2014

[D.S.Mahra]
AOR for petitioner(s)/appellant(s)

SYNOPSIS

The Petitioner is aggrieved by the order dated 26.02.2014 passed by the High Court of Bombay at Goa in Criminal Writ Petition No.10 of 2014 wherein the petitioner had challenged an order dated 22.10.2013 passed by Judicial Magistrate First Class, Vasco Da Gama wherein upon an application made under Section 91 of CrPC by the respondent, the Ld. Magistrate had directed the petitioner authority to provide the respondents with biometrics of all the residents of Goa enrolled in the UIDAI – Aadhaar scheme for the purposes of investigation in a criminal case pertaining to rape of a minor student in Goa. Challenging the said order of the JMFC, the petitioners filed Criminal Writ Petition No.10 of 2014 praying for quashing and setting aside of the said order of JMFC.

However vide the impugned interim order passed in the afore-mentioned Criminal Writ Petition, incorrectly stating the submission of the petitioner, the High Court erroneously observed that petitioner had agreed to test the competence of its data base (instead of software/ current technology/ systems in place) in comparing

chance finger prints given in electronic form with the data base of the petitioner. The Court further directed Director-General, Central Forensic and Scientific Laboratory (CFSL), New Delhi to appoint an expert to ascertain from the petitioner's data base whether the data base of the petitioner has the technological capability for matching the chance fingerprints electronically obtained with its data base. The Petitioner was also given the opportunity to obtain a report from any expert deemed fit by the petitioner. Report of both the experts was directed to filed within two weeks. Further the Court held that the legal aspect of right to information and right to privacy would be considered by it subject to the ultimate decision of this Hon'ble Court in Justice K.S. Puttaswamy v. UOI (Writ Petition (C) No.494/2012) which is still pending.

However the said impugned interim order will have major ramifications on the petitioner Authority especially since the question of law involved in the same, i.e. whether data provided by the residents can be shared without their consent and the related issue regarding a resident's right to privacy is still under

consideration before this Hon'ble Court by way of Writ Petiton (C) No.494 of 2012 titled Justice K.S. Puttaswamy &Anr. v. UOI &Ors. and other connected matters. Permitting a third party to test the veracity of the petitioner's data base and technology/ software in absence of any such defined rules and regulations especially when the issue whether such data can be shared in the first place, is still pending for determination before the Hon'ble Apex Court, is completely erroneous and violates the basic mandate given to the petitioner Authority which collected this vast data base on the solemn assurance that the same shall not be parted with and shared without the consent of the residents.

It is brought to the notice of the Hon'ble Court that the database referred to in the impugned order is backed by a Biometrics de-duplication technical application. If anything, It is the latter that needs to be assessed for its ability to undertake forensic checks and applications and its reliabilityfor taking up matches from a chance fingerprint.

Furthermore, if this Hon'ble Court, in Writ Petition (C) No.494 of 2012 subsequently decides and affirms the stand of the petitioner Authority that biometric data cannot be shared without the consent of the resident, the entire process of obtaining and examining independent reports from experts as per the impugned order, would be an exercise in futility.

28.01.2009: The Petitioner No.1 Authority came into existence vide Notification No. Notification No-A-43011/02/2009-Admn. I dated 28.01.2009.

21.10.2013: The respondent no.1 moved an application under section 91 of CrPC, being Criminal Misc. Appln. No.172/2013/C in Case No. RC 7(S)/2013/CBI/ACB/Goa being investigated by itwhich involved rape on a minor girl-student in the school premises in Vasco, Goa. It was contended that for the purposes of investigation in the afore-mentioned

F

case, certain palm impression had been obtained from the scene of crime. The respondent by way of the said application requested the JMFC to direct the petitioners herein to provide data base including biometrics of persons from Goa who had enrolled with the petitioner authority so the biometrics of residents could be compared with those obtained from the scene of crime.

22.10.2013: The Ld. Judicial Magistrate, First Class passed an ex-parte order dated 22.10.2013 wherein it was observed that since the information sought was important for further investigation in the case and also considering the nature of the case, it directed DG, UIDAI, New Delhi and Dy. DG, UIDAI Technology Centre, Bangalore, to provide the necessary data to Respondent.

23.10.2013: That pursuant to the aforesaid order, the Petitioner received a letter dated

G

23.10.2013 from The Deputy Superintendent of Police, CBI, Anti-Corruption Branch, Goa requesting it to provide data available in the data base of UIDAI, including fingerprints, of three persons whose name and address has been detailed in the said letter.

December 2013: The petitioner challenged the aforesaid order of JMFC dated 22.10.2013 by way of Criminal Writ Petition No.10 of 2014 for quashing and setting aside the order dated 22.10.2013 passed by the Ld. Judicial Magistrate, First Class.

04.02.2014: Notice was issued in the Criminal Writ Petition No.10 of 2014. Further operation of the impugned order passed by JMFC was stayed for two weeks.

24.02.2014: During the course of hearing, the Counsel for petitioner submitted that the current software/ technology/

systems used by UIDAI did not permit authentication of data using only chance/ latent fingerprints. It was further submitted that the request of the respondent no.1 in demanding from the petitioner to compare chance finger prints with the biometric data already available was not only legally untenable on the yardstick of constitutional safeguards and beyond the mandate of the petitioner Authority, but the same was also technically not possible given the current software implementation . The UIDAI system is designed and built to de-duplicate biometrics of enrolled residents using 10 fingerprints, 2 iris, and 1 facial image captured on a computer client machine specially designed and developed by UIDAI called 'Aadhaar Enrolment Client ' with extensive quality and compliance checks. De-duplication requires multi-

modal (including ten finger prints, two iris and face) fusion scoring. Searching theentire database using a few partial fingerprints, that too latent prints having moderate/poor quality or quality specifications not matching with those captured at UIDAI's Aadhaar Enrolment Client machines, could potentially produce lakhs of false matches due to its fundamental nature. This means any such random search, which was now being demanded by the Respondent No.1, even if implemented in the current system, would put lakhs of innocent people under the scanner.

It was also informed to the Court that the current system, including de-duplication sub-system, has functional capability to de-duplicate only from the biometric images created using the Aadhaar Enrolment Client. This means that in order to search using latent/

chance fingerprints on a disc,several parts of the current Aadhaar system would need to be changed, re-designed, re-built, and the entire de-duplication system re-tuned and expanded to include forensic search features. Building a system that can search using latent fingerprints, quite like criminal database searches, is not within the constitutional and legal mandate and scope of UIDAI and fundamentally against the core reason for which the residents have provided their data voluntarily to UIDAI.Time was however sought on the said date by the counsel for respondent no.1 to seek necessary instructions.

26.02.2014: Vide the impugned interim order, the Hon'ble High Court, incorrectly stating the submission of the petitioner, erroneously observed that petitioner had agreed to test the competence of its

data base (instead of software/ current technology/ systems in place) in comparing chance finger prints, given in electronic form, with the data base of the petitioner. The Court further directed Director-General, Central Forensic and Scientific Laboratory (CFSL), New Delhi to appoint an expert to ascertain from the petitioner's data base whether the data base of the petitioner has the technological capability for matching the chance fingerprints electronically obtained with its data base. The Petitioner was also given the opportunity by the Hon'ble Court to obtain a report from any expert deemed fit by the petitioner. Reports of both the experts were directed to be filed within two weeks. In the same order the Hon'ble Court also held that the legal aspect of right to information and right to privacy would be considered

by it subject to the ultimate decision of this Hon'ble Court in Justice K.S. Puttaswamy v. UOI (Writ Petition (C) No.494/2012) which is still pending. Further , in the absence of any clear Terms of Reference for undertaking any such assessmentof thedatabase and its ability, it is humbly submitted that no purpose shall be served.

Further, in the absence of any clear Terms of Reference for ascertaining the technological capability for matching such chance fingerprints without compromising the privacy and security of the CIDR, and without permitting or undue access to the CIDR. No purpose shall be served.

13.3.2014: Hence the present Special Leave Petition.

IN THE HIGH COURT OF BOMBAY AT GOA
CRIMINAL WRIT PETITION NO.10 OF 2014

UNIQUE IDENTIFICATION AUTHORITY
OF INDIA THROUGH ITS DIRECTOR
GENERAL AND ANR. ....Petitioners

Versus

CENTRAL BUREAU OF INVESTIGATION ....Respondents

Mr. Ravi Prakash, Ms. Udita Singh and Mr. H. D. Naik, Advocates for the petitioners.
Mr. Joseph Vaz, Special Public Prosecutor for the respondent no.1.
Mr. A.N.S. Nadkarni, Advocate General with Mr. D. Lawande, Additional Public Prosecutor for the respondent no.2.

Coram:- SMT. R. S. DALVI &
F. M. REIS, JJ.
Date:- 26th February, 2014

P.C.

Rule.

2. Mr. Joseph Vaz, learned Special Public Prosecutor waives notice on behalf of the respondent no.1 and Mr. D. Lawande, learned Additional Public Prosecutor waives notice on behalf of the respondent no.2.

3. The petitioner who is Unique Identification Authority of India itself has sought to challenge the order of the learned Magistrate dated 22.10.2013

passed for providing certain data to the CBI upon an application of the CBI under Section 91 of the Criminal Procedure Code.

4. The application shows the purpose of obtaining the necessary data; it is in respect of investigation in the case of a rape of seven years old child who was the school student and in which case the incident transpired in a school toilet by an unknown person during the recess time on a given date.

5. The CBI has certain chance fingerprints obtained from the place of the incident. It was the case of the CBI that thumb impression available with the petitioner could be compared with the chance fingerprints obtained by the CBI to trace the accused.

6. The investigation is yet in progress. The accused is not traced. The petitioner has refused to co-operate. The petitioner has challenged the order of the learned Magistrate for providing the necessary data for further investigation.

7. The petitioner has taken up the legal contention of privacy not of itself, but of the various applicants and other card holders, if such information is to be provided. It is argued on behalf of the petitioner that the impugned order is cryptic and without any reason and hence it is required to be set aside.

8. The petitioner has relied upon the judgment of in the case of District Registrar and Collector Vs. Canara Bank and others, (2005) 1 SCC 496 in which the parameters for providing information which would not infringe the privacy of any individual is being considered. The judgment also mentions the prarametres and the limits of providing information with the reasons and objectives for an application in that behalf. The Supreme Court has considered the law relating to unreasonable searches and seizures, arbitrary inference with the privacy of family Court and correspondence and unreasonableness qua the right of the persons in exercising their privacy. In that case the documents from certain financial institutions, bank etc

which were asked for by the Government authority were refused as they transgressed those parametres.

The Supreme Court laid down the necessity of reasonable and warranted searches and seizures to be made which would not violate the fundamental rights under Article 20(3) of the Constitution of the India.

9. In this petition, we would have to see from the observations of the Supreme Court whether the fingerprints required for the purpose of further investigation in a case of a rape by an unknown person upon a minor child could be obtained by the CBI. The petitioner has informed the Court that there are number of petitions pending before the Supreme Court and which are being heard along with the main petition no.494/2012 under Article 32 of the Constitution of India filed by Justice K. S. Puttaswamy Vs. Union of India. Copies of the various petitions are filed before us today.

10. The CBI initially required the entire data available of all the persons in the State. That request was

modified and only the fingerprints of three specified persons were required. The petitioner refused to provide the information. CBI has obtained independent information by obtaining fingerprints of those persons. Those persons are now not wanted by the CBI as those fingerprints have not matched with the chance fingerprints taken by the CBI. Thereafter the CBI has sent a letter to the petitioner enclosing the CD containing a soft copy of the chance fingerprints and requested the petitioner to compare its data with the bio-metric data furnished by the CBI.

11. It is contended by the petitioner that it is impossible in view of their limited competence. Counsel on behalf of the petitioner stated that they are incompetent to have any comparison of the data with what is in the data base based upon such bio-metric information as their software does not permit such comparison.

12. Learned Advocate General and counsel on behalf of the CBI have stated to Court that the chance

fingerprints obtained by the CBI can be compared with the limited data base of other investigating agencies.

13. Counsel on behalf of the petitioner has agreed to test the competence of the petitioner's data base in comparing the chance fingerprints given in electronic form with the data base of the petitioner.

14. In view of the statement of the learned Advocate General and counsel on behalf of CBI that the CBI and other investigating agency that their limited data base can scan and match the chance fingerprints with the fingerprints in their data base, a report in that behalf about the capability of the data base software of the petitioner would be required. The petitioner has no objection for obtaining a report in that behalf.'

15. The learned Advocate General states that Director General of Central Forensic and Scientific Laboratory(CFSL), CGO Complex, Lodhi Road, New Delhi can appoint an expert to ascertain from the petitioner's data base also in New Delhi whether the data base of the petitioner has the technological

capability for matching the chance fingerprints electronically obtained with its data base.

16. The petitioner also offers to give names of the experts known to the petitioner to give such a report.

17. Report from the expert appointed by Director General of CFSL as also the report from any expert deemed fit by the petitioner may be filed before this Court.

18. Both the experts shall file their report within two weeks from today. The legal aspect of the right to information and right of privacy shall be considered by the Court subject to ultimate decision of the Supreme Court in the above petition and other petitions pending before it.

19. Stand over 18.3.2014.

SD/-
F. M. REIS, J.

SD/-
SMT. R. S. DALVI, J.

//TRUE COPY//

IN THE SUPREME COURT OF INDIA

CRIMINAL APPELLATE JURISDICTION

(UNDER ARTICLE 136 OF THE CONSTITUTION OF INDIA)

SPECIAL LEAVE PETITION (CRI) NO. OF 2014

BETWEEN **POSITION OF THE PARTIES:**

	Before Trial Court	Before High Court	Before this Court
1. UNIQUE IDENTIFICATION AUTHORITY OF INDIA Through its Director General Having Headquarters at Planning Commission, Government of India, 3rd Floor, Tower II Jeevan Bharti Building, Connaught Circus New Delhi – 110001	Respondent No.1	Petitioner No.1	Petitioner No.1
2. Deputy Director-General, UIDAI Technology Centre, Bangalore	... Respondent No.2	Petitioner No.2	Petitioner No.2

Versus

1. Central Bureau of Investigation, Anti-Corruption Branch, Goa Through Dy. Superintendent of Police	Petitioner	Respondent	Respondent
2. State of Goa Through its Principal Secretary Goa Secretariat Goa.	Not a party	Respondent No.2	Respondent No.2

Both are contesting respondents.

AND IN THE MATTER OF:

SPECIAL LEAVE PETITION UNDER ARTICLE 136 OF THE CONSTITUTION OF INDIA AGAINST THE IMPUGNED INTERIM ORDER DATED 26.02.2014, PASSED BY THE HIGH COURT OF BOMBAY AT GOA IN CRIMINAL WRIT PETITION NO. 10 OF 2014

TO,

THE HON'BLE THE CHIEF JUSTICE OF INDIA AND HIS OTHER COMPANION JUDGES OF THE HON'BLE SUPREME COURT OF INDIA.

HUMBLE PETITION OF THE PETITIONER ABOVENAMED:

MOST RESPECTFULLY SHEWETH:-

1. That the present is a petition under Article 136 of the Constitution of India for grant of Special Leave to Appeal to the petitioner herein against the Impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa in Criminal Writ Petition No. 10 of 2014 preferred by the petitioners challenging the order dated

2. That in order to appreciate the various contentions raised by the petitioner herein, it is necessary to state the following few facts in brief:

(i) The Petitioner No.1 Authority came into existence vide Notification No. Notification No-A-43011/02/2009-Admn.I

dated 28.01.2009. A true copy of the said notification dated 28.01.2009 is annexed herewith and marked as **Annexure P-1. [Page No. 42 to 46].** UIDAI as an authority has been created by the above executive order as an Attached Office under the Planning Commission to ensure a pan-departmental and neutral identity for the Authority and at the same time enable a focused approach to attaining the goals set for the XI Plan in its initial days. A True copy of the Process Committee minutes which recommended the basic structure of UIDAI dated nil is annexed herewith and marked as **Annexure P-2 [Page No. 47 to 53]**

3. The UIDAI has been constituted by the Government of India as an "Attached office" of the Planning Commission by an executive order and its functioning is fully backed by statutes. It has been assigned responsibilities under the Government of India (Allocation of Business Rules) in exercise of the powers conferred by Clause (3) of Article 77 of the Constitution. The Planning Commission, the parent body of UIDAI has amongst other business has the following business:

a) Formulation of Plan for the most effective and balanced utilisation of the country's resources.

b) Definition of stages in which the Plan should be carried out on a determination of priorities and allocation of resources for completion of each stage.

c) Determination of the nature of the machinery necessary for the implementation of the Plan in all its aspects.

d) Identifying the factors which are tending to retard economic development and determine the conditions which, in view of current social, and political situation, should be established for the successful execution of the Plan.

e) Appraise from time to time the progress achieved in the execution of each stage of the Plan and recommend adjustment of policies and measures that such appraisal may show to be necessary.

f) Public Co-operation in National Development.

g) Specific programmes for area development notified from time to time.

h) Perspective planning &

i) Unique Identification Authority of India (UIDAI) –

a. Policy, planning and implementation of Unique Identification Number (UID) for residents in India and all matters related to it.

Unique Identification Authority of India (UIDAI) and connected matters.

As an Attached Office of Planning Commission, the mandate of UIDAI is to be within the ambit of above and it

does not include any forensic or criminal investigative mandate. A Copy of the Government of India (Allocation of Business Rules) in exercise of the powers conferred by Clause (3) of Article 77 of the Constitution dated nil is annexed herewith and marked as **Annexure P-3.[Page No. 54 to 61]**

4. It is humbly submitted that the UID project is a complex technology project designed to support e-governance in the country. The implementation of the project itself as well as its usages by other agencies ensures process re-engineering on a substantial scale. In particular manual process and manual database need to be replaced by electronic process and electronic data bases. Supporting administrative arrangements for programme implementation also need to be recast to reap the full benefits of efficiency, transparency, accountability and economy of the resultant egovernance.It is submitted that Aadhaar is a randomly generated 12-digit unique number which the UIDAI issues to all residents in India on a voluntary basis. The number is stored in a secure database and linked to the basic demographics and biometric information – photograph, ten fingerprints and iris – of each individual. It is verifiable in an online, cost-effective way.

5. The random number generated is devoid of any classification based on caste, creed, religion and geography. Further, to ensure uniqueness of the individual, it has been made essential that the bio-metrics captured are as per the specifications laid down by the Bio-metrics Standards Committee. A Copy of the Bio-metrics Standards Committee report dated nil. is annexed herewith and marked as **Annexure P-4....[Page No. 62 to 160]**

6. The Petitioner would like to submit the background of the UIDAI scheme further to emphasize that developmental purposes of the programme. The UID scheme is envisaged as a means to enhance the delivery of welfare benefits and services. Before the advent of UID Scheme, there has been no single document which was uniformly acceptable as proof of identity across India – irrespective of age, gender and familial connections. Thus establishing identity has always been a challenge for the poor, particularly when they move from place to place, and as a consequence, lack of proof of identity makes it difficult for the poor to access benefits and services. Hence enrolling for the UID or the Aadhaar may be the first form of identification they will have access to.

7. Aadhaar-Pro-poor Approach

An important public policy imperative for introduction of Aadhaar was the understanding of the

Government that a very large number of residents, primarily the poorest, are not able to access services and benefits intended for them for want of being able to prove their identity to service providers and agencies that dispense them. It is well known that notwithstanding the provisions of Law, the birth of close to half the population in many States is never registered. A large percentage of people do not have a birth certificate, the primary document used to prove identity and citizenship.

An inclusive design for enrolment into Aadhaar was therefore deliberately adopted by the Government of India. It was decided that Aadhaar will prove identity and not citizenship given the difficulty the vast majority, particularly the poor, would have in proving their citizenship credentials in the absence of birth certificate or passport. Based upon the recommendations of an expert Committee as contained in its report, "Demographic Data Standards and Verification Procedure Committee Report" dated 09.12.2009, the Government adopted the suggested process of verifications to be followed for enrolment of residents into the Aadhaar system. Accordingly, three distinct methods of verification for obtaining Aadhaar have been adopted:

- Based on supporting documents
- Based on Introducer system
- Based on National Population Register process of public scrutiny.

Each of these methods is well considered, provides for robust verification following a due process and leaves a permanent trail, electronically captured, detailing the entry of each and every individual into the system.

A copy of the "Demographic Data Standards and Verification Procedure Committee Report" dated nil is annexed herewith and marked as **Annexure P-5. [Page No. 161 to 196]**

8. Enrolment of residents with proper verification is a key concern of the UIDAI and for this purpose it ensures proper verification of their demographic and biometric information. As a part of its pro-poor approach the UIDAI focuses on enrolling India's poor and under privileged community for many of whom Aadhaar may be the first form of identification but no one gets enrolled for Aadhaar without undergoing the prescribed method of verification.

Aadhaar – An Enabler for identity verification

It is submitted that Aadhaar number is an enabler. The benefits of Aadhaar number are:—

For residents: The Aadhaar number will become the single source of identity verification. Once residents enroll, they can use the number multiple times – they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on. The number will also give migrants mobility of identity.

For Registrars and enrollers: The UIDAI will only enroll residents after de-duplicating records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower Know Your Resident (KYR) costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate.

The strong authentication that the Aadhaar number offers will improve services, leading to better resident satisfaction.

For Governments: Eliminating duplication under various schemes is expected to save the Government exchequer a substantial amount. It will also provide Governments with accurate data on residents, enable direct benefit programs, and allow Government departments to coordinate investments and share information.

With Aadhaar number integration in various Government schemes, the identity of the beneficiary gets established, by which it is ensured that the government scheme benefits reach the intended beneficiaries. Availability of identity and eligibility information together provides an important tool to plug the loopholes in the eligibility determination process, and in managing the eligibility life cycle for a beneficiary.

9. The use of Aadhaar in being initiated gradually for selected government programmes in districts which have a high coverage of Aadhaar and exception management system has been put In place to ensure that there is no denial of services for want of Aadhaar. Special arrangements have also been put in place for beneficiary of government programmes to obtain Aadhaar expeditiously without difficulty. This is consistent with the stated policy of

government to use Aadhaar for inclusion of the poor and marginal section of society into the fold of social security programme.

Central Government Ministries using Aadhaar based Identity systems:

1. Ministry of Petroleum and Natural Gas
2. Ministry of Social Justice and Empowerment
3. Ministry of Human Resources (Department of Higher Education)
4. Ministry of Human Resources (Department of School Education and Literacy)
5. Department of Tribal Affairs
6. Department of Minority Affairs
7. Ministry of Women and Child Development
8. Ministry of Health and Family Welfare
9. Ministry of Labour and Employment

State Governments Involvement and Usage of Aadhaar based Identity System:

1. Andhra Pradesh
2. Chandigarh
3. Delhi
4. Haryana
5. Jharkhand
6. Karnataka

7. Madhya Pradesh
8. Maharashtra
9. Puducherry
10. Punjab
11. Rajasthan
12. Himachal Pradesh
13. Sikkim

These Ministries/Department have 28 beneficiary programmes using Aadhaar based Identity systems. Some other achievements are as follows:

a) 292banks which have had Aadhaar beneficiary transactions.

b) 300 banks are currently live on Aadhaar Payment Bridge (APB). Details of these banks arranged in alphabetical order dated nil is annexed and marked as **Annexure P-6.[Page No. 197 to 202]**

c) More than **25.6 people** have received their MGNREGS wages/ pensions using Aadhaar online authentication services in March 2014 alone. This system is being used by India Post and banks.

d) As on date, **6.33 crore** people have bank accounts linked to Aadhaar thus making them ready to receive any subsidy/ welfare payment by the Government.

These facts are brought to the notice of the Hon'ble Court to emphasize the socio-economic and developmental mandate associated with UIDAI, rather than any surveillance or forensic application.

The introduction of Aadhaar needs to be seen in the same vein and as a part of the continuing quest of the Government to improve efficient and transparent delivery of public services.

However, for providing social security benefits and subsidies which are discretionary in nature there cannot be any lawful objection for the Government to insist on the use of Aadhaar to ensure the benefits reach only the entitled persons as also to plug wasteful and fraudulent leakages.

10. Aadhaar has been designed specifically to assist in meeting these ends. The Government of India recognizes it as a strategic policy tool for social inclusion, public sector delivery reform and for managing the fiscal deficit. The importance and utility of Aadhaar for delivery of public services has also been recognized by this Hon'ble Court in WP(C) No.196/2001, *PUCL Vs. Union of India* vide order

dated 14.09.2011 as well its judgement as in Civil Appeal No.958/2013 dated 6.2.2013, *State of Kerala & Others Vs. President, Parents Teachers Association, SNVUP and Others*. Copies of these judgments are annexed herewith as **Annexure P-7 (Colly)..[Page No.203 to 238]**

11. The Aadhaar scheme is primarily a developmental initiative and its design features, enumerated above, have been arrived at with the express purpose of improving delivery of social security benefits and subsidies, plugging leakages and wastes, eliminating fakes and duplicates and enhancing transparency and accountability.

The scheme has the approval of the Union Cabinet and its funding requirements are being met year after year with the approval of the Parliament under the Appropriation Act. The application of Aadhaar to the social security benefit programmes of the Government is clearly in the larger public interest.

12. The UIDAI is collecting bare minimum demographic information from the residents such as name, age, gender, address and relationship details in case of minors, photograph alongwith biometric information of ten fingerprints and Iris. This is the information the that UIDAI requires to provide a de-duplicated and unique identity to the residents. As stated previously,the collection of biometrics was based on the recommendation of the

Biometrics Standards Committee Report. It is further submitted that the UIDAI biometric system design has followed global best practices, and in designing this biometric system, UIDAI reviewed existing state-of-the-art biometric systems, consulted with the world's top biometric experts, conducted a Proof of Concept study and built a biometric system that is currently considered to be world's largest and the best. UIDAI has also regularly measured and published empirical and verifiable results. Reviews of the facts and the measures of the live production system are in stark contrast with the claims made about efficacy and accuracy of biometrics system. A summary of details are as follows:

- In December of 2009, UIDAI Committee on Biometrics published its report titled "Biometric Design Standards for UID Applications".

  The Committee acknowledged that most other large-scale biometrics deployments were fingerprint-only and a fingerprint-based system may present challenges in India due to large number of people engaged in agriculture and other manual labour intensive occupations. The committee therefore held extensive meetings and discussions with international experts and technology providers. A technical sub-group analysed fingerprint data collected from Delhi, UP, Bihar, and Orissa and found

that the quality of the data was not substantially different from those collected in western countries. The committee said that it is possible to improve the accuracy of fingerprint system by additionally using iris. *"Iris can provide accuracy comparable to fingerprints. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy"*. The final biometric committee report for this study concluded: "The biometric accuracy levels necessary for de-duplication of all residents of India are achievable".

13. It is submitted that the UIDAI system has been developed for civilian use and for non-forensic purposes and that the implications of False Positive Identification Rate (FPIR)of 0.057%, based on the collection of data in accordance with prescribed standards, arrived at and documented inRole of Biometric Technology in Aadhaar Enrollment report,applied in the UIDAI database of 60 crore residents,will imply a false matches of lakhs of residents that may emerge. It is submitted that this FPIR rate is attainable only under standard controlled conditions by a willing resident using a certified biometric equipments which enables the deduplication system to undertake this task. In other cases being heard in the Supreme Court wherein UIDAI has contented to according regard to security and privacy

aspects towards residents data and its ability to issue de-duplicated identity in accordance with prescribed standards and procedures.

A true copy of the Role of Biometric Technology in Aadhaar Enrolment report dated Nil. is annexed herewith and marked as **Annexure P-8 [Page No.239 to269]**

UIDAI, in view of the above has not been mandated to act as a reservoir of biometric database to assist or undertake forensic activities and neither to go down that path.

14. On 21.10.2013, the respondent no.1 moved an application under section 91 of CrPC, being Criminal Misc. Appln. No.172/2013/C in Case No. RC 7(S)/2013/CBI/ACB/Goa being investigated by itwhich involved rape on a minor girl-student in the school premises in Vasco, Goa. It was contended that for the purposes of investigation in the afore-mentioned case, certain palm impression had been obtained from the scene of crime. The respondent by way of the said application requested the JMFC to direct the petitioners herein to provide data base including biometrics of persons from Goa who had enrolled with the petitioner authority so the biometrics of residents could be compared with those obtained from the scene of crime. A true copy of Criminal Misc. Appln.No.172/2013/C in Case No. RC 7(S)/2013/CBI/ACB/Goa dated 21.10.2013 is annexed

herewith and marked as **Annexure P-9. Page No. 270 to 272]**

15. The Ld. Judicial Magistrate, First Class passed an *ex-parte* order dated 22.10.2013 wherein it was observed that since the information sought was important for further investigation in the case and also considering the nature of the case, it directed DG, UIDAI, New Delhi and Dy. DG, UIDAI Technology Centre, Bangalore, to provide the necessary data to Respondent. A true copy of order dated 22.10.2013 passed by the Ld. JMFC in Crl. Misc. Appln No.172 of 2013/C is annexed herewith and marked as **Annexure P-10... Page No. 273 to 274]**

16. That pursuant to the aforesaid order, the Petitioner received a letters dated 23.10.2013 from The Deputy Superintendent of Police, CBI, Anti-Corruption Branch, Goa requesting it to provide data available in the data base of UIDAI, including fingerprints, of three persons whose name and address has been detailed in the said letter. cissued by respondent no.1 is annexed herewith and marked as Annexure **P-11 (Colly). Page No. 273 to ___]**

17. The petitioner challenged the aforesaid order of JMFC dated 22.10.2013 by way of Criminal Writ Petition No.10 of 2014 for quashing and setting aside the order dated 22.10.2013 passed by the Ld. Judicial Magistrate, First

Class. A true copy of Criminal Writ Petition No.10 of 2014 is annexed herewith and marked as **Annexure P-12 Page No. 277 to 320]**

18. Notice was issued in the Criminal Writ Petition No.10 of 2014 on 04.02.2014. Further operation of the impugned order passed by JMFC was stayed for two weeks. A true copy of order dated 04.02.2014 passed by the High Court of Judicature at Bombay Bench at Goa in Cr. W. P. No.10 of 2014 is annexed herewith and marked as **Annexure P-13. Page No. 321]**

19. During the course of hearing on 24.02.2014, the counsel for petitioner, by way of a rejoinder – affidavit, submitted that the current software/ technology/ systems used by UIDAI did not permit authentication of data using only chance/ latent fingerprints. It was further submitted that the request of the respondent no.1 in demanding from the petitioner to compare chance finger prints with the biometric data already available was not only legally untenable on the yardstick of constitutional safeguards and beyond the mandate of the petitioner Authority, but the same was also technically not possible given the current software implementation. True copy of the letter dated 13.3.2014 is annexed as **Annexure P-14 Page no.322 to 326).** The UIDAI system is designed and built to de-duplicate biometrics of enrolled residents using 10

fingerprints, 2 iris, and 1 facial image captured on a computer client machine specially designed and developed by UIDAI called 'Aadhaar Enrolment Client' with extensive quality and compliance checks. De-duplication requires multi-modal (including ten finger prints, two irises and face) fusion scoring. Searching entire database using a few partial fingerprints, that too latent prints having moderate/poor quality or quality specifications not matching with those captured at UIDAI's Aadhaar Enrolment Client machines, could potentially produce lakhs of false matches due to its fundamental nature. This means any such random search, which was now being demanded by the Respondent No.1, even if implemented in the current system, would put lakhs of innocent people under the scanner. This has been detailed Paras above.

The UIDAI's Biometric Standards Committee constituted by UIDAI which was headed by Director General NIC (National Informatics Centre), published a report in December 2009 had the following assertion on the forensic application:

> *'From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.'*

20. In its Strategy Overview, UIDAI has clearly stated that the UIDAI will not share resident data. The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity onlythrough a 'Yes' or 'No' response. The Authentication system whereby a Resident provides his fingerprint or iris and then enters his Aadhaar number ensure that CIDR of UIDAI can undertake 1:1 match. The success of authentication based on biometrics is therefore based on standardizedprocess and the resident being available or live fingerprint rather than partial or chance fingerprint. On the other hand, UIDAI processes requires all ten fingerprints and iris to undertake 1:N match and de-duplication.

A true copy of "Strategy Overview" dated Nil. is annexed herewith and marked as **Annexure P-15... Page No. 327 to 379]**

21. UIDAI is capturing biometrics and demographics information to issue Aadhaar numbers to the residents and to authenticate the identity of an Aadhaar number holder. It is the responsibility of UIDAI and its Registrars to ensure

safety and security of the data collected for Aadhaar enrolment. A true copy of "Data Protection and Security Guidelines for Registrars" dated nil. is annexed herewith and marked as **Annexure P-16... Page No. 380 to 397]**

22. UIDAI has subscribed to the general principles and procedures relating to data collection, use and processing and these include the following guidelines for the Registrars:

- *Registrars must collect information from residents only for the purpose related to their functions.*
- *The individual from whom data is being collected should be informed of the purpose for which information is being collected and how the data will be used.*

In view of the above, where more than 60 crore residents have enrolled for Aadhaar by providing their demographic and biometric information, sharing of their data based on technology and programme that is for civilian application will probably lead to FALSE MATCH and has the possibility of endangering the Fundamental rights of number of residents

23. Further, it is submitted humbly that the Right to Privacy is one of the basic human right of an individual and UIDAI is committed to protect this aspect. In principle, UIDAI has followed the following general principles associated with

the privacy aspects related to data of the residentenrolling for Aadhaar. These are as

i. Notice to Residents: At the time of enrolment, the resident is aware of enrolling to get an ID and address proof.

ii. Choice and Consent: Explicit consent (in writing or electronically authenticated) of resident is sought to share data for availing welfare services, enrolment itself is voluntary, use of Aadhaar is always consent driven and all data is encrypted at source, biometrics are anonymised even for de-duplication purpose .

iii. Data Collection: Minimal information collected and that too only with the consent of the resident

iv. Purpose Limitation: Data collected only for issue of Identity and Address Proof, explicit consent sought for any other use, resident can withdraw consent, data shared only with resident consent and retained data is encrypted and secure

v. Access and Corrections: The Resident has/will have access to his authentication records and the Self Service Updation Portal and permanent Enrolment Centres provides the Resident with an opportunity to update his

information. This will include choice to the Resident to review the consent he had provided earlier.

vi. Disclosure of Information: UIDAI never discloses resident data except with explicit consent of the resident, entities with whom data is shared with resident consent are required to maintain security standards and disclosure to law enforcement is only in accordance with law.

vii. Security: The UIDAI has implemented state-of- the- art and strict data security architecture and processes to ensure security and confidentiality of resident data.

viii. Openness: Simple and transparent enrolment process, full visibility of data recorded to the resident at the time of enrolment

ix. Accountability: The IT Act provides for an accountability framework, which will be strengthened by the proposed NIDAI Bill

24. The data sharing, privacy and confidentiality issues of database of the residents information is maintained by the following processes adopted by UIDAI:The Residents is required to provide his consent at the time of enrolment based on which residnets data is shared with the agencies involved with welfare services.

The NIDAI Bill has the following provisions on maintenance of data sharing and security aspects of resident data:

Clause 23 (2)(k) of the Bill provides for sharing information of Aadhaar number holders, with their written consent, with such agencies engaged in delivery of public benefits and services as the Authority (UIDAI) may, by order, direct. There may be instances where the resident gives the consent through other means, including electronic means.

Clause 30 of the NIDAI Bill is reproduced below, which is indicative of the data confidentiality being ensured by UIDAI.

- Clause 30. (1) The Authority shall ensure the security and confidentiality of identity information and authentication records of individuals.
- (2) The Authority shall take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof.
- (3) Notwithstanding anything contained in any other law and save as otherwise provided in this Act, the Authority or any of its officer or other employee or any agency who maintains the Central Identities

Data Repository shall not, whether during his service as such or thereafter, reveal any information stored in the Central Identities Data Repository to any person,

Provided that an Aadhaar number holder may request the Authority to provide access identity information in such manner as may be specified by regulations.

25. The High Court was also informed that the current system, including de-duplication sub-system, has functional capability to de duplicate only from the biometric images created using Aadhaar Enrolment Client. This means that to search using latent/ chance fingerprints on a disc, several parts of the current Aadhaar system need to be changed, re-designed, re-built, and entire de-duplication system re-tuned and expanded to include forensic search features. Building a system that can search using latent fingerprints, quite like criminal database searches, is not within the constitutional and legal mandate and scope of UIDAI and fundamentally against the core reason residents have provided their data voluntarily to UIDAI.. Time was however sought on the said date by the counsel for respondent no.1 to seek necessary instructions.

26. Vide the impugned interim order dated 26.02.2014, the Hon'ble High Court, incorrectly stating the submission of

the petitioner, erroneously observed that petitioner had agreed to test the competence of its data base (instead of software/ current technology/ systems in place) in comparing chance finger prints given in electronic form with the data base of the petitioner. The Court further directed Director-General, Central Forensic and Scientific Laboratory (CFSL), New Delhi to appoint an expert to ascertain from the petitioner's data base whether the data base of the petitioner has the technological capability for matching the chance fingerprints electronically obtained with its data base. The Petitioner was also given the opportunity to obtain a report from any expert deemed fit by the petitioner. Report of both the experts was directed to file within two weeks. Further the Court held that the legal aspect of right to information and right to privacy would be considered by it subject to the ultimate decision of this Hon'ble Court in Justice K.S. Puttaswamy v. UOI (Writ Petition (C) No.494/2012) which is still pending Based on the impugned order of the court, the CFSL has already approached the petitioner on 12.03.14 to ascertain the technical capability of the UIDAI for matching the change /finger print obtained petitioner has responded to the CFSL pointing out the directions of the High Court related to and seeking information on the proposed mythology by their expert. True copy of the letter dated 13.3.2014 is annexed as **Annexure P-17..[Page No. 398**

the petitioner, erroneously observed that petitioner had agreed to test the competence of its data base (instead of software/ current technology/ systems in place) in comparing chance finger prints given in electronic form with the data base of the petitioner. The Court further directed Director-General, Central Forensic and Scientific Laboratory (CFSL), New Delhi to appoint an expert to ascertain from the petitioner's data base whether the data base of the petitioner has the technological capability for matching the chance fingerprints electronically obtained with its data base. The Petitioner was also given the opportunity to obtain a report from any expert deemed fit by the petitioner. Report of both the experts was directed to file within two weeks. Further the Court held that the legal aspect of right to information and right to privacy would be considered by it subject to the ultimate decision of this Hon'ble Court in Justice K.S. Puttaswamy v. UOI (Writ Petition (C) No.494/2012) which is still pending Based on the impugned order of the court, the CFSL has already approached the petitioner on 12.03.14 to ascertain the technical capability of the UIDAI for matching the change /finger print obtained petitioner has responded to the CFSL pointing out the directions of the High Court related to and seeking information on the proposed mythology by their expert. True copy of the letter dated 13.3.2014 is annexed as **Annexure P-17.. [Page No. 398**

to 399] Also, it is humbly submitted that as a part of a large policy dialogue, the limitation of the CIDR of UIDIA for investigation purposes have been brought to the notice of the CBI, the respondents. c is annexed herewith and marked as **Annexure P-18.....[Page No. 400 to 401].** It had been brought out in the notice of CBI that the privacyconcerns of the individuals who have voluntarily enrolled for Aadhaar as also the technical architecture of the CIDR of UIDAI, precluderandom bio search. Therefore, the CIDR is not of use for investigative work of CBI.

27. Being aggrieved by impugned interim order, the petitioner approaches this Hon'ble Court by way of the present Special Leave Petition.

28. That the petitioner has not filed any other Special Leave Petition in this Hon'ble Court or in any other Court against the impugned interim order dated 26.02.2014 passed by the High Court of Bombay at Goa in Criminal Writ Petition No.10 of 2014.

29. That the parties herein were parties before the Courts below.

30. That the petitioner prefers the instant Special Leave Petition, amongst others, on the following grounds:

GROUNDS

A. Because in the facts and circumstances of the instant case, the impugned interim order of the High Court cannot be legally sustained as they are contrary to well settled principle of law and as such it is fit to be set aside.

B. Because the impugned interim order resorts to testing the technology of the petitioner with regard to data sharing without the principal issue of data sharing vis- a-vis the fundamental right to privacy of citizens being settled. As has already been mentioned before, the said issue is the subject matter of various petitions filed before this Hon'ble Court challenging the establishment of the petitioner authority. It is pertinent to note here that the lead matter on the issue, being Justice Puttaswamy &Anr. v. UOI (W.P (C) No.494/2012) is as on date being heard by this Hon'ble Court.

C. Because the impugned interim order passed by the Ld. High Court order would have profound implications on the working of UIDAI and acting as a precedent, would open floodgates of similar requests being placed upon the petitioner by various investigative agencies/ police calling for information,

including biometrics of residents for the purposes of investigation.

D. Because it had been the case of the petitioners all along, including its submissions made before the High Court that it can, in no manner, part with biometric data without the consent of the resident as the same would be against the mandate of the petitioner. The current data sharing policy and guidelines upon which the petitioner authority functions clearly provides that biometric data cannot be shared without the consent of the resident. This is the reason for the consistent refusal by the petitioner authority to share data in the absence of consent for the same being obtained from the requisite resident. A true copy of the Data Sharing Policy in use by UIDAI dated nil is annexed herewith and marked as **Annexure P-19... Page No. 402 to 408]**

E. Because the impugned order further suffers from various inaccuracies in as much as despite submissions to the effect being made by the counsel for the petitioner, the impugned order records that the petitioner agrees to test the competence of its *data base* in comparing chance fingerprints which is completely incorrect. On the contrary, the petitioner

had submitted that due to the current software/ systems in place being used by it for authentication of data, comparison of chance fingerprints cannot be done using the current/ existing software. However the order at several places records that it is UIDAI's data base which is not capable, which was never the submission made before the Court.

PRAYER

It is, therefore, most respectfully prayed that your Lordships may graciously be pleased to:

(i) Grant Special Leave to Appeal to the Petitioner herein against the impugned interim order dated 26.02.2014 of the High Court of Bombay at Goa passed in Criminal Writ Petition No.10 of 2014;

(ii) Pass such other order or orders as this Hon'ble Court may deem fit and proper in the facts & circumstances of the case as well as in the interest of justice.

AND FOR THIS ACT OF KINDNESS THE HUMBLE PETITIONER AS IN DUTY BOUND SHALL EVER PRAY.

DRAWN BY: FILED BY:

[Zohaib Hossain] [D.S.Mahra]

ADVOCATE ADVOCATE FOR THE PETITIONER

DRAWN ON: .03.2014

FILED ON: .03.2014

IN THE SUPREME COURT OF INDIA
[CIVIL APPELLATE JURISDICTION]

SPECIAL LEAVE PETITION (C) No. of 2014

IN THE MATTER OF: -

UNIQUE IDENTIFICATION AUTHORITY OF INDIA & ANR.. ..PETITIONERS

VERSUS

CENTRAL BUREAU OF INVESTIGATION & ANR. ..RESPONDENT

CERTIFICATE

CERTIFIED that the Special Leave Petition is confined only to the pleadings before the Court whose order is challenged and the other documents relied upon in those proceedings. No additional facts, documents or grounds have been taken therein or relied upon in the Special Leave Petition. [Except Annexure:P-12 with separate Application for permission to file Additional Documents]. It is further certified that the copies of the documents/annexures, attached to the Special Leave Petition are necessary to answer the questions of law raised in the petition or to make out grounds urged in the Special Leave Petition for consideration of this Hon. Court. This certificate is given on the basis of the instructions given by the petitioner/person authorised by the petitioner whose affidavit is filed in the support of the Special Leave Petition.

[D.S.MAHRA]
Advocate for the Petitioners.

FILED ON: 13.03.2014

IN THE SUPREME COURT OF INDIA
[CIVIL APPELLATE JURISDICTION]

SPECIAL LEAVE PETITION (C) No. of 2014

IN THE MATTER OF: -

UNIQUE IDENTIFICATION AUTHORITY OF INDIA & ANR.. ...PETITIONERS

VERSUS

CENTRAL BUREAU OF INVESTIGATION & ANR. ..RESPONDENT

AFFIDAVIT

I, Ashish Kumar, Assistant Director General, Having Office of Planning Commission Government of India, 3rd Floor, Tower II Jeevan Bharti Building, Connaught Circus New Delhi - 110001, do hereby solemnly affirm and state as under: -

1. That I am working as Assistant Director General, Having Office of Planning Commission Government of India, 3rd Floor, Tower II Jeevan Bharti Building, Connaught Circus New Delhi - 110001 of the petitioner department and as such I am fully conversant with the facts and circumstances of this case, hence I am competent to swear this affidavit.

2. That I have read and understood of the contents of the accompanying List of Dates B to L and paragraphs 1 to 8 of the Special Leave Petition at

pages 08 to 39 and Crl.M.Ps. and say that the facts stated therein are true to my knowledge derived from official records and information received and believed to be true. The legal submissions are verified as true based upon Legal advice received by me and believed to be true.

3. That the Annexures are the true copies of the respective originals and are essential parts of the records.

DEPONENT

VERIFICATION:

I the above named deponent do hereby verify that the contents of the above affidavit are true and correct to the best of my knowledge and belief and nothing material has been concealed therefrom.

Verified at New Delhi dated this 13th Day of March, 2014.

DEPONENT

42

ANNEXURE P-1

(TO BE PUBLISHED IN PART-I, SECTION-2 OF THE GAZETTE OF INDIA)

GOVERNMETN F INDIA

PLANNING COMMISSION

Yojana Bhawan Sansad Marg New Delhi, 28 January,2009

NOTIFICATION

No. A-4301 1102/2009.Admn. I: In pursuance of Empowered Group of Ministers' fourth meeting, dated 4 November 2008, the Unique Identification Authority of India (UIDAI) is hereby constituted and notified as an attached office under aegis of Planning Commission within following terms of reference and initial core staff composition:-

COMPOSITION

2. UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:

Post	Level	No. of Posts
UID Authority of India		
Director General & Mission Director	Additional Secretary Govt. of India	1
Deputy Director General (DDG)	Joint Secretary, Govt. of India	1
Assistant Director General (ADG)	Director, Govt. of India	1
Support Staff		

PS	PS	3
Peon	Peon	2
Driver	Driver	2
	Total Manpower	10
State/UT Units of UIDAI		
State UT UID Commissioner	Joint Secretary, govt. of India	35
Support Staff		
PS	PS	35
Peon	Peon	35
	Total Manpower	105
	Grand Total	115

Role and Responsibilities of UIDAI

3. UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and operate UID database and be responsible for its updation and maintenance on an ongoing basis

4. Implementation of UID scheme will entail, inter alia, following responsibilities being undertaken by UIDAI:

- Generate and assign UID to residents
- Define mechanisms, and processes for interlinking UID with partner databases on a continuous basis.
- Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis.

- Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism.
- Define usage and applicability of UID for delivery of various services.
- Operate and manage all stages of UID lifecycle.
- Adopt phased approach for implementation of UID especially with reference to approved timelines.
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages, across partner agencies as well as its validation while cross linking with other designated agencies.
- Evolve strategy for awareness and communication of UID and its usage.
- Identify new partner /user agencies.
- Issue necessary instructions to agencies that undertake creation of databases, to ensure

- Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism.
- Define usage and applicability of UID for delivery of various services.
- Operate and manage all stages of UID lifecycle.
- Adopt phased approach for implementation of UID especially with reference to approved timelines.
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages, across partner agencies as well as its validation while cross linking with other designated agencies.
- Evolve strategy for awareness and communication of UID and its usage.
- Identify new partner /user agencies.
- Issue necessary instructions to agencies that undertake creation of databases, to ensure

standardization of data elements that ace collected and digitized and enable collation and correlation with UID and its partner databases.

- Frame policies and administrative procedures related to hiring / retention/ mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all. State units under UIDAI.

5. Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning arid budgetary support. Planning commission would provide initial office and IT infrastructure at central level.

6. Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development. Secretary to the Government of India.

Sd/-
(Dr.Subas Pani)
Secretary to the Government of India

The General Manager
Govt. of India Press
Faridbad,

Copy to:

1. Secretary to the President, Rashtrapati Bhavan, New Delhi.

2. Secretary to the Vice-President, Maulana Azad Road, New Delhi

3. Cabinet Secretary, Rashtrapati Bhavan, New Delhi.

4 Principal Secretary to the Prime Minister, South Block, New Delhi

5. Private Secretary to the Deputy Chairman, Planning Commission

6. All Ministers/Departments of Govt of India

7. Chief Secretaries of all States/Union Territories

8. Secretary General, Rajya Sabha Secretariat, New Delhi

9. Secretary General, Lok Sabha Secretariat, New Delhi

10. Pr. Adviser (Admn. & PC)/AS & FA/ Adviser (C& I) /Director (GA)/DS (Admn.)

11. Pay & Accounts, Officer Planning Commission

12. Drawing & Disbursing Officer, Planning Commission

13. Accounts-I Section Planning Commission,

//TRUE COPY//

47

ANNEXURE:P-2

Planning Commission

(C&I Division)

MINUTES OF THE SIXTH MEETING OF THE PROCESS COMMITTEE ON PROJECT UID HELD ON 15th JUNE 2007

LIST OF PARTICIPANTS IS AT ANNEXURE.

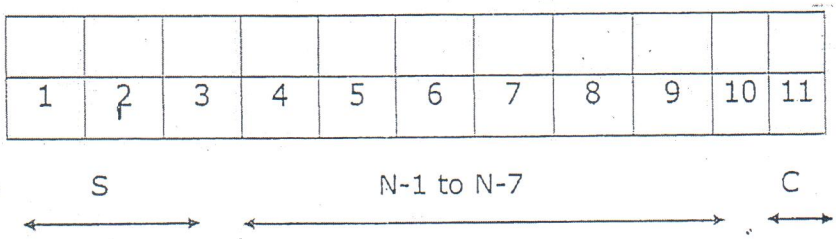
The Sixth meeting was held on 15th June under the Chairmanship of Dr. Arvind Virmani, Principal Adviser (Planning Commission). The meeting commenced with a presentation by the process study consultants. M/s Wipro, covering all aspects that were discussed in the last meeting of the Committee Following was the agenda set by the Committee and covered by the consultant:

1. Revised numbering format
2. UID Governance Structure
3. Proof of Concept (PoC) Status
4. Phasing Plan (Tentative)

1. Numbering Format

2. The revised proposal arrived at, (after deliberation with DG(NIC) and RGI) recommending a 11 digit numbering format, was explained to the Committee.

Briefly stated, it proposed that the 11 digit number would be:



S1-S3: Number Allocation Series for State (000-999) 1 Crore Series

N1: N7: Serial Number (00001-99999)

N1-N2: For series allocation to Districts by the State (00-99) 1 Lac Series.

C: Checksum Digit (Algorithm used Modulus 10)

3. The first three digits of the numbering format (S1-S3) as one crore series would be mapped with states and next two digits with district as one Lac series in the database. Initially the districts would be mapped centrally and shared with the states and any later addition /amendments may be left to the states (to be carried out as per control rules that would be laid down centrally).

4. UID would remain same for lifetime of a resident and there would be no re-allocation of UID number.

2. ULD Governance Structure

5. After discussions in this regard, it was decided to set up an independent UID authority under the ageis of Planning Commission and it was felt that a cabinet note would accordingly be drafted for this purpose in due course.

6. The overall Resource requirement in the ULD governance structure would evolve over time/phases across functions. It was suggested by the Committee that in the initial stage of the governance structure, critical senior administrative levels may have to be filled on deputation, and other options such as contractual employment, outsourcing etc. may be explored for filling in operational levels.

3. Proof of Concept (PoC) - Status

7. The Committee was briefed on the status and initial findings of the proof of Concept exercise being undertaken by Wipro at five locations for UID-BPL, UID-PDS and UID-EC linkage.

8. A team of officials from EC, PDS and other departments (both serving and retired) who are involved

in carrying out the PoC exercise in the field gave their observations and findings on feasibility of establishing the linkage of UID with partner databases and elaborated on the related issues.

9. The committee appreciated the findings of the PoC, which clearly established the feasibility of linkage between UID and partner databases. It was apprised to the Committee that the team could successfully match and incorporate UID in 85% (UID-BPL and UID-PDS) records in partner databases in rural areas. In urban areas, matching of records percentage is relatively less.

10. It was stated that M/S Wipro would submit their final PoC report for all 5 locations by June end.

4. Phasing Plan (Tentative)

11. A phased approach has been proposed for adoption of UID by states and partner Departments, wherein the UID authority would play a critical role in finalizing the modalities and timelines. The first step would be the generation of UID numbers and creation of the UID authority under the Planning Commission.

51

12. The Committee was apprised of the ground covered in the meetings with ECI and the modalities that are being worked out for linkage with EC. ECI would be the first partner database to be linked with the UID database. Linkage with MoRD and POS would happen subsequently and in phased manner.

Decisions taken by the Committee

I. The revised numbering format as proposed, was approved by the Committee.

II. The Committee appreciated the need for the UID authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the authority and at the same time enable a focused approach to attaining the goals set for the XIth Plan.

III. Proposal for creation of Central and State UID authorities and riding on the existing administrative (revenue) set up for operation and coordination at district and sub district level was approved.

IV. Consultants to provide details of the sourcing and staffing for UID authority (central and state) in

initial and subsequent phases along with financial implications.

V. PoC observations/findings were appreciated by the Committee for linkage with partner databases. Consultants to submit final report on PoC by June end.

VI. DIT to work out modalities for linkage with EC and initiate discussions with MoRE and PDS for linkage.

VII. Committee indicated 'in principle' approval of the proposed sequence for the phasing plan:

- generation of UID,
- creation and notification of Central and State UID Authorities under the Planning Commission.
- establish ongoing linkage of UID with ECI database.
- initiate deliberations on linkage with MoRO and DoF&PD (PDS).

The meeting ended with vote of thanks to the chair.

53

ANNEXURE

LIST OF PARTICIPANTS

PLANNING COMMISSION

1. Dr. Arvind Virmani, Pr. Adviser
2. Shri M.M. Chanda, Joint Adviser (C&I)
3. Shri T.K. Choudhury, S.R.O.

DEPARTMENT OF INFORMATION TECHNOLOGY, ELECTRONICS NIKETAN, 6 CGO COMPLEX, LODI ROAD, NEW DELHI

1. Shri R. Chandrashekhar, Addl. Secretary
2. Smt. Radha Chauhan, Pr. Consultant

NATIONAL INFORMATIC CENTER (NIC), A BLOCK, CGO COMPLEX, LODI ROAD, NEW DELHI.

1. Dr. B.K. Gairola, DG

REGISTRAR GENERAL OF INDIA, 2A, MANSINGH ROAD, NEW DELHI

1. Shri C. Chakraborty, Joint Director
2. Shri Dheeraj Jain, Assistant Director.

WIPRO

1. Shri Himakar, 201/5, Sector-I, Pushp Vihar, New Delhi-17
2. Dr. Anurag Srivastava, Plot No. 480-481, Udyog Vihar, Phase III, Gurgaon – 122016.

//TRUE COPY//

ANNEXURE P-3

THE GOVERNMENT OF INDIA (ALLOCATION OF BUSINESS) RULES

In exercise of the powers conferred by clause (3) of article 77 of the Constitution and in super session of all previous rules and orders on the subject the President hereby makes the following rules for the allocation of the business of the Government of India.

1. Short Title - These rules may be called the Government of India (Allocation of Business) Rules, 1961.

2. Allocation of Business The business of the Government of India shall be transacted in the Ministries, Departments, Secretariats and Offices specified in the First Schedule to these rules (all which are hereinafter referred to as "departments").

3. Distribution of Subjects –

1. The distribution of subjects among the departments shall be as specified in the Second Schedule to these rules and shall include all attached and subordiate offices or other organisations including

Public Sector Undertakings concerned with its subjects and sub-rules(2), (3) and (4) of this rule.

2. The compiling of the accounts of each Department shall stand allocated to that Department with effect from the date from which the President relieves, by order made under the first proviso to sub-section (1) of Section 10 of the Comptroller and Auditor General's (Duties, Powers and Conditions of Service) Act, 1971; the Comptroller and Auditor General from the responsibility for compiling the accounts of that Department.

3. Where sanction for the prosecution of any person for any offence is required to be accorded-

1. If he is a Government servant, by the Department which is the Cadre Controlling authority for the service of which he is a member, and in any other case, by the Department in which he was working at the time of commission of the alleged offence.

2. If he is a public servant other than a Government servant, appointed by the Central Government, by the Department administratively concerned with the

organisation in which he was working at the time of commission of the alleged offence and

3. In any other case, by the Department which administers the Act under which the alleged offence is committed; Provided that where, for offences alleged to have been committed, sanction is required under more than one Act, it shall be competent for the Department which administers any of such Acts to accord sanction under all such Acts.

4. Notwithstanding anything contained in sub-rule (3), the President may, by general or special order, direct that in any case or class of cases the sanction shall be by the Department of Personnel and Training.

4. Allocation of Departments among Ministers –

1. The business of the Government of India allocated to Cabinet Secretariat is and, shall always be deemed to have been, allotted to the Prime Minister.($)

2. Subject to the provisions of sub-rule (1), the President may, on the advice of the, Prime Minister, allote the business of the Government of India among Ministers by assigning one or more departments to the charge of a Minister.

3. Notwithstanding anything contained in sub-rule(1) or sub-rule(2), the President may, on the advice of the Prime Minister –

1. Associate in relation to the business allotted to a Minister under either of the said sub-rules, another Minister or Deputy Minister to perform such functions as may be assigned to him or

2. Entrust the responsibility for specified items of business affecting any one or more than one Department to a Minister who is in charge of any other Department or to a Minister without Portfolio who is not in charge of any Department.

RAJENDRA PRASAD

PRESIDENT

//TRUE COPY//

Substituted by 116th Amendment of the "Rule" on 29th March, 1976. # sub-para 391) substituted and sub-paras 3(30 and 394) inserted by 187th Amendment of the "Rules" on 30th September, 1986. ($) Substituted by 87th Amendment of the "Rules" on 26th October, 1970. *# Substituted by 271 Amendment of the "Rules" on 6th January, 2004.

//TRUE COPY//

PLANNING COMMISSION (YOJANA AYOG)

1. Assessment of the material, capital and human resources of the country, including technical personnel, and formulation of proposals for augmenting such of these resources as are found to be deficient.

2. Formulation of Plan for the most effective and balanced utilisation of the country's resources.

3. Definition of stages in which the Plan should be carried out on a determination of priorities and allocation of resources for completion of each stage.

4. Determination of the nature of the machinery necessary for the implementation of the Plan in all its aspects.

5. Identifying the factors which are tending to retard economic development and determine the conditions which, in view of current social, and political situation, should be established for the successful execution of the Plan.

6. Appraise from time to time the progress achieved in the execution of each stage of the Plan and recommend

adjustment of policies and measures that such appraisal may show to be necessary.

7. Public Co-operation in National Development.

8. Specific programmes for area development notified from time to time.

9. Perspective planning.

10. Institute of Applied Manpower Research.

11. The overall coordination of the Pradhan Mantri Gramodaya Yojana.

Note: The overall coordination of the Pradhan Mantri Gramodaya Yojana (PMGY) will be the responsibility of the Planning Commission. However, overall management and monitoring of the individual sectoral programmes under PMGY will be the responsibility of the concerned nodal Ministry/Department.

12. Unique Identification Authority of India (UIDAI)-

(a) Policy, planning and implementation of Unique Identification Number (UID) for residents in India and all matters related to it.

(b) Unique Identification Authority of India (UIDAI) and connected matters.

13. All matters relating to National Rainfed Area Authority (NRAA).

//TRUE COPY//

62

Annexure-24

Biometrics Design Standards

For

UID Applications

Version 1.0

December 2009

Prepared by: UIDAI Committee on Biometrics

UIDAI

63

CONTENTS

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable.

These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

The Committee however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never

been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context.

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in

developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy.

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion.

Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.

2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be

consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.

3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.

4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.

5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by

incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.

6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.

8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is

necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards,, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

3 Objective

The UIDAI bio metrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.

- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.

· To specify design parameters of the standards that will be used for the UID system.

· To estimate the accuracy achievable using different biometric modalities in the
Indian environment.

· To make recommendations to the UIDAI on the use of biometric modalities. From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations.

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997

ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6.3. Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022. (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

7 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in India, the Committee

selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

Figure 1 ISO Biometrics Standards Activity

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured.

8.1.1 For Enrollment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

Face Image Type Code	Scan resolution (dpi)	Color Space Code	Source Type Code	Inter-eye distance (pixels)	Facial Expression Code
Full Frontal (0x01)					

300 24 bit RGB

(0x01)

0x02

0x06

120 0x01

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

16.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

16.1.4 Pose

Roll, pitch and yaw angle should not be more than ±50 (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

16.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBEFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document.

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8.3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

9 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

9.1 Section 7: Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images

be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

9.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel

depth

(bits)

Dynamic

range

(gray levels)

Certifications

31 197 500 8 200 EFTS/F

9.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

Setting

level

Scan

resolution

(ppcm)

Scan

resolution

(dpi)

Pixel

depth

(bits)

Dynamic

range

(gray levels)

Certifications

281 118 300 4 12 UID

30 197 500 8 80 None

9.2 Section 8 Finger Image record Format

9.2.1 Section 8.2.14 Image compression algorithm

9.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

9.2.1.2 Authentication

Code 4, compressed – JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

1 Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification

of this standard in bitmap is 7.5MB per subject.

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1.3 Impression Type

For enrolment image, only code2 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not indented to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

2 Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND-VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color

Digital/Photographic requirements

R, S Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2.

Inter-eye distance – minimum 120 pixels.

Pose S Per ISO 19794-5 Section 7.2.2

Expression R, S Neutral expression. Specified as best practices.

Illumination S Per ISO 19794-5 Section 7.2.7

Eye Glasses S Per ISO 19794-5 Section 7.2.11

Accessories R Permissible for medical and ethical reasons only.

Multiple samples of face

M Yes. Recommended for automatic face recognition.

Operational S Per ISO 19794-5 Section 7.2.4 - 7.2.10

Assistance R Yes. Specified as best practices.

Segmentation and

feature extraction

M Recommended for automatic face

recognition

Quality check R Yes. Specified as best practice.

Storage & compression S Uncompressed image strongly

recommended. For legacy reasons,

lossless JPEG 2000 color accepted.

Authentication

Image capture R Same as enrollment

Compression S JPEG 2000 color compression

recommended. Compression ratio to

be less than 10:1.

Number of Images R One full frontal image

Figure 2 Face image

12.2 Fingerprint.

Key Decisions Decision

Type3

Summary of Decisions

Enrolment

Image capture

Plain or rolled R Plain, live scan

Number of fingers R Ten

Device characteristics S Setting level 31 or above, EFTS/F certified

Quality check R Yes – specified as best practice

Operational

Assistance R Yes – Specified as best practice

Corrective measure R Yes – Specified as best practice

Storage & transmission

Compression S Uncompressed images strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.

Storage format S Per ISO Section 8.3. No deviation necessary

Minutiae format S Per ISO 19794-2. No deviation necessary.

Multi-finger fusion algorithm

R Recommended. Application dependent.

Authentication

Image capture

Number of fingers R No minimum, no maximum. Application dependent. Recommended as best practice

Any finger option M Yes. Recommended as best practice

Retry R Maximum 5. Recommended as best practice.

Device characteristics S Setting level 28 or above

Transmission format S Per ISO. No tailoring necessary

Compression S JPEG 2000 compression recommended.

Compression ratio to be less than 15:1

Minutiae format S Per ISO 19794-2. No tailoring necessary

Figure 3 Fingerprint

3 R: Recommendation based on best practice/empirical data, S: Standard based, M:

Management judgment.

12.3 Iris

Decision Decision Type

Summary of Decision

Enrolment

Image R Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and

right, 25% top and bottom of iris diameter

Device Characteristics R Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control

Operational M Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor.

Segmentation R Non-linear segmentation algorithm

Quality Assessment R Per IREX II recommendations4

Compression & Storage S ISO 19794-6 (2010) data format standard as tailored in Section 11.

JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).

Authentication R, S Same as enrollment except One or two eyes

JPEG 2000

KIND_CROPPED of Table A.1

Figure 4 Iris

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

4 IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality

on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes.

Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggestthat quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.

2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.

3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.

4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

· Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can besuperior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.

· In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions. · The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

13 Members

13.1 Biometrics Committee

Name, Affiliation

1. Dr. B. K. Gairola, DG NIC – Chairman
2. Dr. C. Chandramauli – Registrar General of India (RGI) – Member
3. Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member
4. Dr. A. M. Pedgaonkar, RBI – Member
5. Mr. Pravir Vohra, ICICI – Member
6. Prof. Deepak Phatak, IIT Bombay – Member
7. Prof. Phalguni Gupta, IIT Kanpur – Member

8. Mr. R. S. Sharma, DG UIDAI – Member/Convener

9. Mr. Rajesh Mashruwala, UIDAI – Member

10. Mr. Srikanth Nadhamuni, UIDAI – Member

13.2 Face Sub-committee

1. Dr. Richa Singh

2. Dr. Mayank Vatsa

3. Mr. Rajesh Mashruwala

13.3 Fingerprint Sub-committee

1. Prof. Phalguni Gupta

2. Dr. A. M. Pedgaonkar

3. Mr. Rajesh Mashruwala

4. Dr. Mayank Vatsa

13.4 Iris Sub-committee

1. Prof. Phalguni Gupta

2. Dr. Mayank Vatsa

3. Mr. Rajesh Mashruwala

Annexure I

Notification of UIDAI constituting the Committee

Annexure II Technical Data

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all therequirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible[1].

Demographic data is used along with the biometric information to improve the deduplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in deduplication.

It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general,

it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images.

Fingerprints also lend themselves very well to forensic investigation. There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or

more fingers [5]. Fingerprint technology constitutes approximately half of the total biometrics market5.

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired.

Iris has no association with law enforcement and has not received negative press andmay therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of theiris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user

cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

Biometric identifier

Reference FRR FAR

Fingerprint NIST FpVTE 0.1% 1%

Face NIST FRVT 10% 1%

Voice NIST 2004 5-10% 2-5%

Iris ITIRT 0.99% 0.94%

Figure 5 FAR and FRR error rates

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

Key Decisions Type	Decision
Summary of Decisions	
Enrolment	
Image capture requirements	R Full frontal, 24 bit color
Inter-eye distance	minimum 120 pixels.
Digital/Photographic	R, S Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical

Corrigendum 2.

Pose S Per ISO 19794-5 Section 7.2.2

Expression R, S Neutral expression. Specified as best practices.

Illumination S Per ISO 19794-5 Section 7.2.7

Eye Glasses S Per ISO 19794-5 Section 7.2.11

Accessories R Permissible for medical and ethical reasons only.

Multiple samples of face

M Yes. Recommended for automatic face recognition.

Operational S Per ISO 19794-5 Section 7.2.4 - 7.2.10

Assistance R Yes. Specified as best practices.

Segmentation and feature extraction

M Recommended for automatic face recognition

Quality check R Yes. Specified as best practice.

Storage & compression S Uncompressed image strongly

recommended. For legacy reasons,

lossless JPEG 2000 color accepted.

Authentication

Image capture R Same as enrollment

Compression S JPEG 2000 color compression

recommended. Compression ratio to be

less than 10:1.

Number of Images R One full frontal image

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection(by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance isrequired. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or

body part (hand, arms) of the assisting person or any object appear in the photograph.

Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devicesto constitute the enrolment station. A tethered biometrics device provides severaladvantages over a stand-alone device. First, it allows the images to be associated withenrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

Pose

Face image should be full frontal with 00 of yaw, pitch and roll angles. However, in operational conditions, variation of ±50 is permissible.

Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses.

However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons.

Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints,

automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image with yaw, pitch and roll angle as 00. The other two images should be left and right semi profile with yaw as ±200 to ±300, and the roll and pitch should be 00.

Operational

Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction

Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check

Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression

According to Figures 12 and 13 of ISO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10.

Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

Authentication

The authentication process consists of steps similar to enrolment.

Image Capture

Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression

For verification, images with JPEG 2000 compression ration of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?

2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?

3. Manage ment judgment (M): Management decision based on project context. The remaining section has a brief explanation of each decision.

Key Decisions	Decision Type
Summary of Decisions	
Enrolment	
Image capture	
Plain or rolled	R Plain, live scan
Number of fingers	R Ten
Device characteristics	S Setting level 31 or above, EFTS/F certified
Quality check	R Yes – specified as best practice. Avoid

NFIQ quality 4 and 5 level fingerprints.

Operational

Assistance R Yes – Specified as best practice

Corrective measure R Yes – Specified as best practice

Storage & transmission

Compression S Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.

Storage format S Per ISO Section 8.3. No deviation necessary

Minutiae format S Per ISO 19794-2. No deviation necessary.

Multi-finger fusion algorithm

R Recommended. Application dependent.

Authentication

Image capture

Number of fingers R No minimum, no maximum. Application dependent. Recommended as best practice

Any finger option M Yes. Recommended as best practice

Retry R Maximum 5. Recommended as best practice.

Device characteristics S Setting level 28 or above

Transmission format S Per ISO. No tailoring necessary

Compression S JPEG 2000 compression recommended.

Compression ratio to be less than 15:1

Minutiae format S Per ISO 19794-2. No tailoring necessary

Figure 7 Fingerprint

Enrolment

The enrolment process can be broken down into image capture ("client") and deduplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the

fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural the maximum possible.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images6. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor.

The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a

NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

6 It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.

2. Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use.

To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not

accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence.

Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for deduplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not

make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

Image capture

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find analternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the

system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very

limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmissionwill contain extracted minutiae. In the second, it will contain the compressed raw image.

For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximumflexibility during authentication. It is understood that raw or compressed image willgive a higher level of accuracy.

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the s erver does not have matching matcher, it will only use "standard" minutiae data.

Iris Image Best Practices

Summary

Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture. Figure 8 summarizes key decisions for UIDAI iris design.

Figure 8 Iris

The remaining section has a brief explanation of each decision.

7 IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

Decision Decision Type	Summary of Decision
Enrolment	

Image R Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter

Device Characteristics R Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control

Operational M, R Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor.

Quality Assessment R Per IREX II recommendations7

Compression & Storage S ISO 19794-6 (2010) data format standard as tailored in Section 11.

JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).

Authentication R, S Same as enrollment except

One and/or two eyes

JPEG 2000

KIND_CROPPED of Table A.1

Enrolment

Iris image

Capture of two eyes simultaneously provides several advantages8. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality. In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a

visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera.

This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the "capture volume") within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range. 8 Material derived from [32]

The iris image capture sensor shall use progressive scanning. In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris.

The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ration of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.

One method widely used for ensuring good iris images is recommended here. An Iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images an d use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming

distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression

(KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

Authentication

For 1:1 verification, any one eye will suffice, though application may require higherlevel assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting imagesize will between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design o f the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade -off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

· Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.

· Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.

2. Estimate difference in image quality between Western and Indian conditions.

3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples.

It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

· False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.

· False Rejection Rate does not vary over gallery size as shown in Figure 12.

· Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of approximately 0.07*200 = 14%. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

· Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

Number of Fingers	FRR %	FAR %
2	10.3	29.2
10	10.9	0.0

Figure 10 Accuracy of multiple fingers

· Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expectedto be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of FAR 1.4% at FRR rate of 2%. In other words, NIST data indicates deduplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or

20% false accept rate).

Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

Figure 14 US-VISIT image quality distribution for right index finger

Figure 15 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained fromdiverse, disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases; fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). This

database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.

2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.

3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software(NFIQ), images were classified in to bins according to the image quality score. The bin distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5

numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

Figure 16 Image quality score distribution for DB1 Urban sample

Figure 17 Image quality score distribution for DB1 Rural sample

Figure 18 Image quality distribution for DB2

Figure 19 Image quality distribution for DB3

Step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, usingexisting Western results[24], it is possible to closely predict the expected fingerprintrecognition performance.

Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Westerncurve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western

curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

Figure 20 Right index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.37%	0.83%	1.31%	2.16%	4.77%
NIST	27.28	33.32	35.37	2.23	1.8
NIST - Cum	27.28	60.6	95.97	98.2	100
DB2	15.87	40.08	28.88	0.99	14.18
DB2 - Cum	15.87	55.95	84.83	85.82	100.00
DB3	49.73	30.51	16.97	2	0.79
DB3 - Cum	49.73	80.24	97.21	99.21	100.00

Figure 21 Right index finger numerical data

Figure 22 Left index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5

0.43% 0.73% 1.24% 2.28% 5.73%

NIST 30.83 29.78 34.08 2.88 2.43

NIST - Cum 30.83 60.61 94.69 97.57 100

DB2 18.99 39.36 25.87 0.90 14.88

DB2 - Cum 18.99 58.35 84.22 85.12 100.00

DB3 57.25 25.77 13.8 1.87 1.31

DB3 - Cum 57.25 83.02 96.82 98.69 100.00

Figure 23 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performanceof fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

· The UIDAI can achieve fingerprint accuracy of a quality similar to developedcountries. There is good evidence to suggest that

Indian rural data may be as good asdeveloped country settings when proper operational procedures are followed andgood quality devices are used.

· It is possible to closely predict the expected fingerprint recognition performance. Inthe experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for Q = 1, 2, and 3, 99% TAR with about 1% FAR).

· It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:

1. Using wet towels to remove dirt and moisten dry fingers
2. Using minimum quality threshold to ensure that extra efforts are made to

capture good prints from hard to obtain fingers and

3. Keeping scanning devices in operational order

These resulted in exceptionally good bin 1 and 2 distribution.

· It is also observed that the slap fingerprint segmentation tools require some priortraining for Indian databases. After some training, segmentation results improve by2-3%. This also suggests that in deploying a biometrics (fingerprint) system, acarefully designed a priori training set and procedure will help in improving performance.

· Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.

· When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub-continental region compared to Western and European countries. Lawsonia Inermis (commonly known as henna or mehandi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and

when applied, fingerprint sensors may not properly capture fingerprint features.

· On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy

using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the later, gallery size is small, typically 1% of database. The hierarchical method improves FRR (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

Iris

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample.

Figure 24 Iris FAR & FRR rate

Figure 25 FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety offields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupt a and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities, combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006

2. Anil Jain, Patrick Flynn, Arun Ross. Handbook of Biometrics, 2008

3. ANSI/NIST-ITL 1-2007. American National Standard for Information Systems— Data Format for the Interchange of Fingerprint, Facial, & Other Biometric

Information – Part 1

4. ANSI/NIST-ITL 2-2008. American National Standard for Information Systems—

Data Format for the Interchange of Fingerprint, Facial, & Other Biometric

Information – Part 2 XML Version

5. Bolle, Connell et al. Guide to Biometrics, 2004

6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft

Version 0.4, National Information Center

7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for

Recognition", Proceedings of International Conference on Signal and Image

Processing (ICSIP 2006), Karnataka, India, 2006

8. IAFIS-IC-0100 (V7) Electronic Fingerprint Transmission Standard (EFTS) 1999

9. International Biometrics Group, "Independent Testing of Iris Recognition

Technology, Final Report, May 2005", NBCHC030114/0002. Study
commissioned by the US Department of Homeland Security.

10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST
Interagency Report 7629

11. ISO/IEC 19784-1:2006. Biometric Application Programming interface – Part1:
BioAPI specification.

12. ISO/IEC 19794-1:2006. Biometric data interchange formats – Part 1: Framework

13. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image
data

14. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris image
data

15. J. Cambier, "Iridian Large Database Performance", Iridian Technical Report 03-
002

16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006

17. J. Daugman, "Iris recognition border crossing system in the UAE", International

Airport Review (2) 2004.

18. J. Daugman, Technical Report 635, University of Cambridge, 2005

19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005

20. Jonathon Phillips, "ICE 2006 Large-Scale Results", NIST 7208, NIST, 2007

21. NISTIR 7110. Matching Performance for the US-VISIT IDENT System Using Flat

Fingerprints. C. L. Wilson, M. D. Garris, & C. I. Watson, May 2004

22. NISTIR 7112. Studies of Plain-to-Rolled Fingerprint Matching Using the NIST

Algorithmic Test Bed (ATB). Stephen S. Wood & Charles L. Wilson, April 2004

23. NISTIR 7123. Fingerprint Vendor Technology Evaluation 2003: Summary of

Results and Analysis Report, Charles Wilson etc al.

24. NISTIR 7151. August 2004 Fingerprint Image Quality.

25. NISTIR 7201. Effect of Image Size and Compression on One-to-One Fingerprint

Matching. C. I. Watson & C. L. Wilson. February 2005

UID Biometrics Design Standards 57 of 57

26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C.

Wilson, M. Indovina & B. Cochran. July 2005

27. NISTIR 7296. MINEX. Performance and Interoperability of the INCITS 378

Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006

28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007

29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures",

IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4,

April 2007.

30. Registry of USG Recommended Biometric Standards, Version 2.0, NSTC

31. Report of the working group on standards for raw images of fingerprints,
Reserve Bank of India

32. Shahram Orandi, . Mobile ID Device Best Practice Recommendations, NIST Special
Publication 500-280, August 2009

33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final
Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific
Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex
TW11 0LW

34. UK Passport Service, Biometrics Enrolment Trial, May 2005

AAIN-P-S
161

Demographic Data Standards and Verification procedure (DDSVP)

Committee Report Version 1.0

December 9, 2009

Prepared by: DDSVP Committee

Unique Identification Authority of India

Planning Commission,

Yojana Bhavan,

Sansad Marg,

New Delhi 110001

CONTENTS

1

162

164

LIST OF TABLES

1 Introduction

UIDAI has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. UIDAI proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identity in order to improve th efficacy of the service delivery. UIDAI has selected biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information is capable of carrying out the de-duplication at the time of collection of information. For government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that the biometric information capture and transmission are standardized across all the partners and users of the UID system.The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of Biometrics,

Personal Identification and location Codification Standards. These committees have worked out standards in the respective categories to be uniformly applied for various egovernance standards. As UIDAI proposes to use common demographic data for establishing and verifying identity, it becomes essential to standardize these fields and verification procedure

across registrars and to aid interoperability across many systems that capture and work with resident identity.

1.1 Definitions and Acronyms

o UID – Unique Identification

o UIDAI – Unique Identification Authority of India

o Authority – Unique Identification Authority of India (UIDAI)

o DDSVP – Demographic Data Standards and Verification Procedure

o KYR – Know Your Resident

o KYC – Know Your Customer

o PoI – Proof of Identity

o PoA – Proof of Address

o DIT – Department of Information Technology

o ORGI – Office of Registrar General of India

o VARCHAR – Variable character string as represented in a database. Unlike the fixedsize character type, VARCHAR does not store any blank characters at the end,
reducing the size of a database when the full length of the field is not used.

o UNICODE – Globally accepted standard definition of local language characters in a
computer system. Character sets defined by Unicode Consortium.

o UTF-8 – Unicode Transformation Format, most widely used storage encoding for any UNICODE data

o Registrar – Any government or private agency that will partner with UIDAI in order to enroll and authenticate residents

o Introducer – A person who is authorized to introduce a resident who does not posses any supporting documents in order to help them establish UID (see later section 3.3 for details)

o Flag – a marker to indicate a particular status of a field

1.2 Committee Objective

A key requirement of the UID system is to capture necessary demographic data in a standardized manner so that this identity information works across various systems.

1. In order to achieve interoperability of data across various govt. and private agencies that will use the UID system, it is important that the capture and verification of basic demographic data for each resident is standardized across all partners of the UID system.

2. Another important aspect of demographic data collection is to ensure the

correctness of the data at the time of enrolment of residents into the UID System. While an elaborate verification system based on local enquiries and existing documents issued by various agencies can be used to verify the correctness of the data to a large degree, it is likely to result into exclusion of poor and the marginalized who normally do not have any documents to prove their identity and addresses. As the main focus of the UIDAI is on inclusion, especially of the poor, the verification procedure has to be formulated in such a manner that while it does not compromise the integrity of the inputs, it also does not result in exclusion and harassment of the poor.

3. The government of India had set up expert committees for standards to be used for various e-governance applications in areas of

Personal Identification, Biometrics, and Location Codification Standards. These committees have worked out few standards on the respective categories to be uniformly applied for various e-governance standards.

4. As UIDAI will use basic demographic data to establish identity and authentication, it becomes essential to review the applicability of the existing data and process standards for various e-Governance applications, modify them for UIDAI specific requirements and frame the methodology for its implementation. In view of the above, a Demographic Data Standards and Verification Procedure (DDSVP) Committee was setup vide OM No.63/DG-UIDAI/2009 dated 09/10/2009 (annexed to this report) to review the existing standards and modify/enhance/extend them so as to achieve the goals and purpose of UIDAI.

1.3 Committee Charter

o To Recommend the Demographic Data standards (The data fields and their formats/structure etc.) that will ensure interoperability and standardization of basic demographic data and their structure used by various agencies that use the UIDsystem. This will necessitate the review of the existing standards of Demographic Data and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI and its partners.

o To Recommend the Process of Verification of these demographic data in order toensure that the data captured, at the time of enrolment of the Residents into the UID system, is correct.

1.4 Target Audience

Any person or organization involved in designing, testing or implementing UID system,UID compatible systems, or UID enrollment for the central government, state government, commercial organizations, or any users of the UID system.

2 KYR Demographic Data

2.1 Introduction

Purpose of UIDAI is to help Residents establish their identity. So, it is important that the KYR data is kept to a usable minimum so as to support goals of UID and avoid other profiling and transactional fields.

2.1.1 Names and Addresses

Names in India can be from a single word to many (sometimes even 5 or more) words long depending on the region, caste, religion, etc. A standardized structure for names needs to be created for common KYR and interoperability between various systems. Similarly, we neither have a standardized address format nor have well defined geographic boundaries beyond villages. This creates issues when trying to map addresses in a standard way. Various forms issued by existing registrars vary greatly when it comes to capturing addresses. As part of this committee, address structure for residents will also be standardized.

2.1.2 UID Number Format

The rationale for adopting UID numbering scheme was explained to the committee by UIDAI which is given below:

UID number is a 12-digit number with no intelligence built into it – it should be a random number, with as few digits as possible to

accommodate the identification needs of the population for the next 100-200 years. UID number will be assigned only after biometric de-duplication process of the data supplied by the registrars.

The following factors were considered in order to arrive at a design of the UID number.

1. The date-of-birth and other attribute information should not be embedded in the UID number. Similarly, place of birth/residence using administrative boundaries (state/district/taluk) should not be embedded in the UID number. When state/district IDs are embedded in the UID number, the number faces the risk of becoming invalid and misleading the authenticator when people move from place to place. It can also lead to profiling/targeting based on the region/state/district that a person is from. The approach of storing intelligence in identification numbers was developed to make filing, manual search and book-keeping easier prior to the advent ofcomputers. This is no longer necessary, since centralized database management systems can index the records for rapid search and access without having to section data by location or date of birth.

2. Given the rapid penetration of mobile phones and landlines across the countryand across economic groups, the phone could become an enabling device used for authenticating a person, especially in the village scenario where internet penetration is still very small. In this case it would be useful to keep the UID number as a number rather than an alphanumeric.

3. Packing Density is the ratio of valid UID numbers issued to the total number of possible UID numbers available given a certain number of digits. The lower the packing density is, the more likely it is that a

random guess will not produce a valid assigned UID number. In general it is suggested that we keep the packingdensity to about 20%.

4. The Authority intends to assign UID numbers to all residents – more than a billion people. UID number will not be re-used and hence numbering scheme need to accommodate necessary population growth over the years.

This committee has taken note of the above.

2.2 UID for Children

All children will be assigned a UID number. It is very important for several service organizations such as education and health to be able identify children uniquely in order to deliver services effectively. Children's' fingerprints are not fully formed and hence cannot be used for de-duplication given current state of technology.

Hence during enrollment, details of the parents are captured in order to link the child to established UIDs so that either of the parents can be used to authenticate the child.When the child's biometrics are well-formed (as per biometric committee recommendations), biometric capture will take place and the child will be de-duplicated to ensure the uniqueness of the child. Until the child is biometrically de-duplicated, theirUIDs will be flagged as "De-duplication not performed".

2.3 Data Fields Summary

Information Fields	Mandatory / Optional	Data Type
Name	Mandatory	Varchar (99)
Date of Birth##	Mandatory	Date
Personal		

Details

Gender Mandatory Char (1) – M/F/T

Address

Details

Residential Address Mandatory 8 address lines and pin code.

See later sections for details.

Father's/Husband's

/Guardian's Name*

Conditional Parent / Varchar (99)

Guardian

Details Father's/Husband's

/Guardian's UID*

Conditional Number (12)

Mother's/Wife's

/Guardian's Name*

Conditional Varchar (99)

Mother's/Wife's

/Guardian's UID*

Conditional Number (12)

Introducer Name** Conditional Introducer Varchar (99)

Details Introducer's UID** Conditional Number (12)

Contact Mobile Number Optional Varchar (18)

Details Email Address Optional Varchar (254)

A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.

** For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory.*

** For children under a particular age, biometric de-duplication will not be done. Hence their UID will be*

flagged as such until they are biometrically de-duplicated at a later age (see section on UID for Children).

Their UID will be linked to at least of the parent's UID.

** For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory. But, an*

option will be provided to not specify in the case the adult is not in a position or does not want to disclose.

*** For residents with no document proof, an "introducer" should certifyhis/her identity. See later sectionon Introducer System.*

Table 1: Data Fields Summary

2.4 Data Fields in Detail

2.4.1 Unique ID

Field Name **UID**

Data Type **Number (12)**

Mandatory / Optional **Mandatory**

Specification Owner UIDAI

Valid Values and

Default Value

Language Support ---

Description Internal generated random number. Unique in the whole system.

Display and Print

Specifications

Print and display format should be NNNN-NNNN-NNNN

2.4.2 Name of Resident

Field Name **NAME**

Data Type **Varchar (99)**

Mandatory / Optional **Mandatory**

Specification Owner DIT (MDDS Standard)

Valid Values and

Default Value

Language Support Yes. Other than English, it will also be stored in one official

Indian language. Data storage will be based in UTF-8. An additional Indian language code (Indian language codes as

UID DDSVP Committee Report Version 1.0 Page 10 of 25

specified under DIT standards) will also be maintained for transliteration purposes. Specific guidelines such as handling "matras" on hand-written forms will be provided by UIDAI as part of registrar on-boarding process.

Description Name of the resident.

Display and Print

Specifications

2.4.3 Date of Birth

Field Name **DOB**

Data Type **Date**

Mandatory / Optional **Mandatory**

Specification Owner DIT (MDDS Standard)

Valid Values and

Default Value

Language Support ---

Description Date of Birth of the resident.

Display and Print

Specifications

Print and display format should be DD/MM/YYYY

2.4.3.1 Date of Birth Type

Field Name **DOB_TYPE**

Data Type **Char (1)**.

Mandatory / Optional **Mandatory**

Specification Owner DIT (MDDS Standard)

Valid Values and

Default Value

"V" - Verified (full DoB as per document)

"D" - Declared (full DoB as declared by resident)

"A" -Approximate (Just the year, based on estimated age)

Language Support ---

Description Flag used to indicate DoB type.

Display and Print

Specifications

2.4.4 Gender

Field Name **GENDER**

Data Type **Char (1)**

Mandatory / Optional **Mandatory**

Specification Owner ORGI

Valid Values and

Default Value

"M" – Male, "F" – Female, and "T" – Transgender

Language Support ---

Description Gender of the resident

Display and Print

Specifications

2.4.5 Residential Address

Field Name **RESIDENTIAL_ADDRESS**

Data Type **Address** (*see address structure details below*)

Mandatory / Optional **Mandatory**

Specification Owner Dept. of Post

Valid Values and

Default Value

Language Support Yes. Other than English, it will also be stored in one official

Indian language. Data storage will be based in UTF-8. An additional Indian language code (Indian language codes as specified under DIT standards) will also be maintained for transliteration purposes.

Description A verifiable address where resident lives normally.

Display and Print

Specifications

Format should be (empty values/lines not printed):

C/o Person Name

Building

Street

Landmark, Locality

Village/Town/City, District

State – Pin Code

2.4.5.1 Address Structure

Address Field Description Data Type Mandatory / Optional

CARE_OF Field to capture "C/o" person name Varchar (60) Optional

BUILDING Door/House/flat/Bldg number and name Varchar (60) Mandatory

STREET Street number and name Varchar (60) Optional

LANDMARK Major/Minor Landmark Varchar (60) Optional

LOCALITY Locality/Area/Suburb/Sector/BlockVarchar (60) Optional

VILLAGE_TOWN_CITY Village/Town/City Varchar (8) for code and Varchar (50) forname (stored ascode*)Mandatory

DISTRICT District Varchar (4) for code and Varchar (50) forname (stored as code*) Mandatory

STATE State Varchar (2) for code and Mandatory Varchar (50) for name (stored as code*)

PINCODE Postal code for a areaCHAR(6) Mandatory

COUNTRY Country. Currentlynot used on forms. Varchar (3) forcode andVarchar (50) forname (stored ascode*) Mandatory

* *All region codes are based on "Land Codification" from ORGI*

2.4.6 Father/Husband/Guardian and Mother/Wife/Guardian Information

Field Name NAME and UID

Data Type Same as Name and UID

Mandatory / Optional **Name** of either Father/Husband/Guardian or Mother/Wife/Guardian **is mandatory for all.** But, **an option will be provided** to not specify in the case the adult is not in a position or does not want to disclose.In the case of **children,** both **Name and UID of at least one parent/guardian is mandatory.**

Specification Owner DIT (MDDS Standard)

Valid Values and Default Value: ---

Language Support Yes. Other than English, it will also be stored in one officialIndian language. Data storage will be based in UTF-8. An additional Indian language code will also be maintained for transliteration purposes.

Description Name and UID of parent/guardian.

Display and Print Specifications---

2.4.6.1 Relationship Type

Field Name **RELATIONSHIP_TYPE**

Data Type **Char (1)**

Mandatory / Optional **Mandatory** when Parent/Spouse/Guardian data is provided Specification Owner UIDAI

Valid Values andDefault Value "F" – Father, "**M**" – Mother, "H" – Husband, "**W**" – Wife, and "**G**" – Guardian

Language Support ---

Description Flag used to indicate. Two separate flags will be stored in database – one for Father/Husband/Guardian and another for Mother/Wife/Guardian. Display and Print Specifications

2.4.7 Introducer Information

Field Name INTRODUCER_NAME and INTRODUCER_UID

Data Type Varchar (99) and Number (12)

Mandatory / Optional **Optional**

Specification Owner UIDAI

Valid Values and

Default Value---

Language Support ---

Description In the case of residents having no documents as proof, they

can be "introduced" by any approved "introducer" (see KYR process chapter for details on introducer system). **Both Name and UID will be captured in form although only Introducer UID will be stored against resident record.**

Display and Print

Specifications

2.4.8 Mobile Number

Field Name **RESIDENT_PHONE**

Data Type **Varchar (18)**

Mandatory / Optional **Optional**

Specification Owner DIT (MDDS Standard)

Valid Values and

Default Value---

Language Support ---

Description Mobile phone number of the resident. This can be used for enhanced authentication and alerting. Landline also will be accepted if mobile number is not available.

Display and Print

Specifications

2.4.9 Email Address

Field Name **RESIDENT_EMAIL**

Data Type **Varchar (254)**

Mandatory / Optional **Optional**

Specification Owner DIT (MDDS Standard)

Valid Values and

Default Value

Language Support Yes.

Description Email address of resident.

Display and Print

Specifications

---

3 KYR Verification Procedure

3.1 Introduction

It is essential that key demographic data is verified properly so that the data within UID system can be used for authentication of identity by various systems. There are 3 distinct methods of verification:

- Based on supporting documents
- Based on introducer system (see section 3.5 for details)
- Based on the NPR (National Population Register) process of public scrutiny

All the above forms of verification are acceptable for UID enrollment.

At a high level the 'Personal Details' and the 'Address Details' are mandatory, whereas the 'Parent/Guardian', 'Introducer' and 'Contact' details are optional or conditional.

In order to verify the correctness of certain mandatory fields, such as Name, date-of birth and address, there is a concept of 'Proof of Identity' (PoI) and "Proof of Address" (PoA). PoI requires a document containing the resident's name and photograph, whereas the PoA contains the name and address.

3.2 Broad Principles of Verification

One of the key goals of the UID system is to be inclusive and ensure every resident is able to establish their identity. There are certain key principles that verification procedure will follow to ensure inclusiveness without compromising data quality.

1. Ease of access
2. No harassment
3. No discrimination
4. No corruption
5. No exclusion

3.3 Verification Summary

Information Fields	Verification Required?	Verification Procedure
Name	Yes	o Any of the PoI documents. o Introducer for people who have no documents.
Date of Birth##	No	---
Personal		

182

Details

Gender No ---

Address

Details

Residential Address

(for UID letter delivery and other communications)

Yes o Any of the PoA documents.

o Introducer for people whohave no documents.

o Address will be physically verified during UID letter delivery. But, resident's physical presence not required during letter delivery. .

Father's/Husband's/Guardian's Name*

Father's/Husband's/Guardian's UID*

Conditional o No verification of

Father/Husband/Guardian in the case of adults.

Mother's/Wife's/Guardian's Name*

Parent /Guardian Details Mother's/Wife's /Guardian's UID*

Conditional o No verification of

Mother/Wife/Guardian in the case of adults.

Introducer Introducer Name**

Details Introducer's UID**

Yes o Introducer's Name, UID on the form.

o Physical presence of the introducer at the time of enrollment may not be

practical. UIDAI will therefore suggest alternate

methods to overcome thispractical difficulty.

Contact Mobile Number No ---

Details Email Address No ---

A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.

** For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory. For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory.*

*** For residents with no document proof, an "introducer" should certify his/her identity. See later section on Introducer System.*

3.4 KYR Guidelines

Following are the main guidelines for KYR process.

- **Uniform process** - A uniform procedure for KYR process & verification to be followed by each registrar that is easy to implement. Once a resident obtains a UID from any one of the registrars in the UID ecosystem; all other registrars will honor the validity of the UID fields obtained through the KYR process described in this document. This can eliminate cost involved in repeated KYR verification by several registrars.
- **Multiple options for supporting documents** - Applicants will be given a choice of supporting documents that they can produce as PoI and PoA. See later sections for supported list of documents.
- **Lack of Supporting Documents** – A process for enrolling residents who have no documented PoI and PoA must be defined through a concept of "Introducer". For details, please see section on Introducer System.
- **orting documents in regional languages** – The UID backend pport the capture and storage of data in 2 languages – fficial Indian language. Enrolling agencies must be

prepared to verify and accept supporting documents that carry information in local languages.

o **Archiving Form & Supporting Documents** – Clarity in how the forms an supporting documents are archived for later access (dispute resolution, error in data entry etc) should be defined and followed across all enrolling registrars. Detail guidelines regarding this will be issued by UIDAI separately.

o **Accepting changes in demographic information** – Some of the fields captured during UID enrollment could change – such as Name and address. An update process will be supported in order to facilitate this. Upon following this process, the registrars will accept changes in demographic details. See later sections for details.

3.5 Introducer System

There are several situations, especially in the case of poor, where they are unable to provide any supporting documents. Since the main goal of UIDAI is inclusion, it is important that an effective process is developed to identify them and give a UID number without harassment. An approach is to use a network of "approved" introducers who can introduce a resident and vouch for the validity of resident's information. Essentially, this idea has been borrowed from the account opening procedure in the banks. When someone opens an account in the bank without any proofs, he/she needs

an "introducer". This introducer is someone who already has an account in the branch and is ready to certify that X who wants to open the account is indeed X. Logically, then a branch has a chain of introducers. Every account that has been introduced is linked to the introducer.

This analogy needs to be generalized and expanded to become applicable to UID registration process. In the UID registration process, registration is proposed to be done through various registrars like the Banks, Insurance Companies, Central and State Government Departments. In each of these institutions, the introducer concept will work like a "tree structure" where one introducer may introduce more than one person.

However, someone needs be the first introducer and be the "root" of this tree. The person at the root will be the person who will be "self-introduced". In other words, that person will be initially registered without any introducer. He will then introduce and get a number of persons registered. This process will then continue. As an example, in a registration process where State's Rural Development Department is the registrar and NREGA is the scheme whose beneficiaries are being registered. In this process, the District Magistrate (or the Deputy Commissioner) can "self-introduce" and become the root of the introducer tree. He/She will introduce his/her BDOs and the Block Panchayat heads (known as Block Pramukhs in some states) who implement NREGA. Each of these BDOs and Block Pramukhs can introduce other people at the Panchayat level like the Panchayat Sewaks, Pradhans/Mukhias (elected Panchayat Head), and ward members (in a village Panchayat). Generally, the last category will reach down to the village level. However, in order to ensure that the enrolment process is not hampered by the lack of approved introducers at the ground level, each registrar should have the freedom to decide on the issue of approved introducers so as to

ensure that there are people at the ground level who are able to introduce the people who want to enroll in the UID system.

Similarly in a banking environment, senior bank officials will be able to introduce the lower functionaries and this will go down to the customer level. In effect, there will be several approved 'introducers' who can help residents without supporting documents to enroll for a UID. Having multiple introducers within and outside government agencies should provide a needy resident access to people who can assert their identity while minimizing harassment. However, the concept of inclusiveness should not take away the credibility of the introducer system. As of now,

offenses of impersonation (by the person) or abatement of this offense (by theintroducer) should therefore be dealt with within the existing legal framework. However, UIDAI should put in place its own legal framework to deal with such situations as early as possible.

3.5.1 Goals of Introducer System

- Provide every resident having no documented proofs to provide an alternate method to confirm their identity and address.
- Ensure availability of multiple introducers so that residents are not being harassed by a single person.
- Since registrars provide the list of introducers, ensure that the introducer network spans people from Govt. and Private (e.g., Banks) and NGO agencies.
- Avoid disputes and fraud by making sure that introducers have their UID created before becoming an introducer and all introducers must be registered as such.

3.5.2 Broad Guidelines for Creating Introducers List

This section covers broad guidelines that can be used by registrars for creating a list of introducers within their domain. Following are some of the guidelines:

o The list of approved introducers should go down till the village/customer level so that the process of registration is not hampered due to lack of introducers.

o The registrars need not keep the hierarchy of approved introducers limited to their own department/organization. As an example, in NREGA, there are a number of NGOs involved in NREGA social audit and the registrars could make some of the representatives of these NGOs who work at the village level as the approved introducers. Similarly, the village teachers and postman could also be incorporated as approved introducers by state Governments if required.

o At the ground level, residents should have access to multiple introducers so as to avoid harassment by a single introducer.

o Introducer list should include credible organizations which have traditionally been advocates of vulnerable communities to make sure goal of inclusion is truly achieved.

3.5.3 Introducer System in Detail

As discussed earlier, UIDAI will request registrars to provide a list of people who can act as trusted introducers within their ecosystem. It is highly recommended that this list includes people from both government and private enterprises including NGOs if necessary so that residents get a choice of people to approach for getting the introduction done. UIDAI may also provide its own list of introducers to make the pool

of introducers large enough. All introducers are required to be enrolled into UID system and obtain their UID number before they can become an introducer. This helps in effectively auditing all introductions.

Residents with no document proofs can approach any of the introducers enlisted to assert their identity. Residents are required to fill up the enrollment form and take it to one of the introducers for getting introduced. Introducer will verify the information filled, fill up his/her name and UID, and put thumb impression within the specified area of the form. UIDAI should, in consultation with its various Registrars, come out with a detailed policy and guideline for the Introducer. This will be in the form of a Manual to be followed by the various stakeholders.

3.6 Supporting Documentation

During enrolment, the quality of data has to be ensured primarily with supporting documents that the resident provides. Copies of documents provided will be verified against the original. Physical copies of the documentary evidence will be stored by the Registrar and available for audit by the designated audit agencies.

In the case of residents with no documentation, introducer system can be used to enroll them into the system.

UIDAI and Registrars shall have the authority to amend and enlarge the list of PoI and PoA documents as and when necessary.

3.6.1 Proof of Identity (PoI) Documents

Proof of Identity document must contain name and photo of the resident. Any of the following PoI documents are supported:

Supported PoI Documents Containing Name and Photo

1. Passport

2. PAN Card

3. Ration/PDS Photo Card

4. Voter ID

5. Driving License

6. Government Photo ID Cards

7. NREGS Job Card

8. Photo ID issued by Recognized Educational Institution

9. Arms License

10. Photo Bank ATM Card

11. Photo Credit Card

12. Pensioner Photo Card

13. Freedom Fighter Photo Card

14. Kissan Photo Passbook

15. CGHS / ECHS Photo Card

16. Address Card having Name and Photo issued by Department of Posts

17. Certificate of Identity having photo issued by Group A Gazetted Officer on letterhead

NOTE: *If any of the above documents submitted do not contain the photograph of the resident, then it will not be accepted as a valid PoI. In order to be inclusive and free of harassment, documents with older photographs are acceptable.*

3.6.2 Proof of Address (PoA) Documents

Proof of Address document **must contain name and address** of the resident. Any of the following PoA documents are supported:

Supported PoA Documents Containing Name and Address

1. Passport

2. Bank Statement/Passbook

3. Post Office Account Statement/Passbook

4. Ration Card

5. Voter ID

6. Driving License

7. Government Photo ID Cards

8. Electricity Bill (not older than 3 months)

9. Water Bill (not older than 3 months)

10. Telephone Landline Bill (not older than 3 months)

11. Property Tax Receipt (not older than 3 months)

12. Credit Card Statement (not older than 3 months)

13. Insurance Policy

14. Signed Letter having Photo from Bank on letterhead

15. Signed Letter having Photo issued by registered Company on letterhead

16. Signed Letter having Photo issued by Recognized Educational Institution on letterhead

17. NREGS Job Card

18. Arms License

19. Pensioner Card

20. Freedom Fighter Card

21. Kissan Passbook

22. CGHS / ECHS Card

23. Certificate of Address having photo issued by MP or MLA or Group A Gazetted Officer on letterhead

24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)

25. Income Tax Assessment Order

26. Vehicle Registration Certificate

27. Registered Sale / Lease /Rent Agreement

28. Address Card having Photo issued by Department of Posts

29. Caste and Domicile Certificate having Photo issued by State Govt.

Table 4: PoA Documents

3.6.3 Proof of Date of Birth (DoB) Documents

Proof of DoB document must contain name and DoB of the resident.

Any of the following documents are supported:

Supported Proof of DoB Documents

1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on letterhead

Table 5: Proof of DoB Documents

3.7 KYR Process

3.7.1 Verifying Name

Name must be verified against any one of the PoI documents listed. A copy of PoI should be kept as part of enrollment and verification should be done against the original document.

In the case of resident not having a valid PoI document, resident should furnish the form signed by any of the approved introducers.

3.7.2 Verification for Name Change

Residents may want to change his/her name due to various reasons. Name change should be verified against documents. Following are the reasons and verification method for supporting name changes.

Marriage

Women may want to change their name after marriage. In this case, a copy of the marriage certificate or any acceptable proof of marriage as approved by the registrar should be provided and should be verified against original documents.

Any Other

Residents may change their name for other reaso ns such as self-wish, religion change, numerology, etc. In all these cases, they should provide a copy of legal name change certificate and it should be verified against the original document.

3.7.3 Verifying DoB

Date of Birth should be verified against any of the Proof of DoB documents listed above. Copy of the document should be verified against the original.In the case of lack of documents, an approximate DoB may be taken and marked as so.

3.7.4 Verifying Address

The addresses will be verified against any one of the PoA documents listed. A copy ofPoA document should be kept as part of enrollment and verification should be done

against the original document. In the case of resident not having a valid PoA document, resident should furnish theform signed by any of the approved introducers.

3.7.5 Verification for Address Change

Residents can update their address through any of the enrolling registrars. Process for address verification is same as described above.

3.7.6 Verifying Parents/Spouse/Guardian Information

In the case children, "Name" and "UID" of one of the parents or guardian is mandatory. Parent/Guardian must bring their UID letter when enrolling children (or they can be enrolled together) and should be verified.

In the case of an adult, no verification will be done for the information on parent or spouse. They are recorded for internal purposes only.

3.7.7 Making Corrections to Initial Data

In the case of mistakes such as spelling errors, address errors, etc. resident should be able to come back and request such corrections. Enrolling agencies should allow makingthose changes based process similar to initial KYR.

3.8 Exceptions Handling

There are likely to be several types of exceptions during enrolment process that need to be handled. Following list provide the common exceptions and appropriate verification method.

DoB Unknown Record estimated year of birth leaving date and month fields. DoB Type flag set to "Approximate".

Inconsistent Address in PoA document

Quite like name spelling errors, address too is likely to have a large number of inconsistencies across documents. Addresses must be mapped appropriately onto the standard KYR address fields as per specification.

Absence of original documents In instances where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.

Table 6: KYR Exceptions List

UIDAI shall have the right to alter / amend the guidelines in this regard from time to time.

4 References

1. "*Person Identification Codification (MDDS), Version 1.02*" – by ExpertCommittee on Metadata and Data Standards, DIT (http://egovstandards.gov.in/).

2. "*Land Region Codification, Version 1.02*" – by Expert Committee on Metadataand Data Standards, DIT (http://egovstandards.gov.in/).

3. "*Master Circular – Know Your Customer (KYC) norms*" – by RBI (http://rbidocs.rbi.org.in/rdocs/notification/PDFs/73IKYC010709_F.pdf)

4. "*UPU S42 International Address Standard*" – by UPU (http://www.upu.int/). Also see the reference article at http://xml.coverpages.org/ni2003-06-17-a.html

5. "*Customer Information Quality Specifications Version 3.0*" – by OASIS (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html)

6. "*Markup Languages for Names and Addresses*" – OASIS Cover Pages (http://xml.coverpages.org/namesAndAddresses.html)

5 Members

5.1 DDSVP Committee

S.No.	Name & Designation	Role
1	Mr. N. Vittal, Former CVC	Chairman
2	Mr. S. R. Rao, Additional Secretary, DIT	Member
3	Dr. C. Chandramauli, RGI	Member
4	Mr. K. Raju, Principal Secretary, Rural Development, GoAP, Hyderabad	Member
5	Dr. DS Gangwar, Jt Secy., Min of Rural Development, NewDelhi	Member

6 Shri Ram Narain, DDG(Security), Dept. of Telecommunication Member

7 Mr. Vinay Baijal, CGM (DBoD), RBI, Mumbai Member

8 Mr. VS Bhaskar, Commissioner & Secretary, Health & FW, IT,Sports & Youth Welfare, Government of Assam, GuwahatiMember

9 Mr. S. Satpathy, Secretary, Rural Development, Govt ofJharkhand, Ranchi Member

10 Ms. Kalpana Tiwari, Department of Posts Member

11 Prof. Bharat Bhaskar, IIM, Lucknow Member

12 Mr. Ashutosh Dixit, Jt. Secretary (TPL II), Dept. of Revenue Member

13 Ms. Madhavi Puri Buch, ICICI Securities, Mumbai Member

14 Dr. Gayathri V., CEO LabourNet Member

15 Mr. Ram Sewak Sharma, DG UIDAI UIDAI Rep.

16 Mr. Srikanth Nadhamuni UIDAI Rep.

17 Dr. Pramod K. Varma UIDAI Rep.

5.2 KYR Data Sub-committee

S.No. Name & Designation Role

1 Shri S.R. Rao, Additional Secy. DIT Chairman

2 Shri Ashutosh Dixit, JS Dept. of Revenue Member

3 Shri Chakravarty DDG, RGI Office Member

4 Dr. D.S. Ganwar, JS, MoRD Member

5 Shri V.S. Bhaskar, Commissioner and Secy, Health and Familywelfare, Govt. of Assam Member

6 Ms. Renu Bhudiraja, Director, DIT Member

7 Ms. Aruna Chaba, Senior Technical Director, NIC Member

10 Shri Ram Sewak Sharma, DG UIDAI UIDAI Rep.

11 Shri Srikanth Nadhamuni UIDAI Rep.

12 Dr. Pramod K. Varma UIDAI Rep.

5.3 KYR Process Sub-committee

S.No.	Name & Designation	Role
1	Ms. Kalpana Tiwari, India Post	Chairman
2	Shri Ram Narain, Joint Secy. DoT	Member
3	Dr. D.S. Ganwar, JS, MoRD	Member
4	Shri V.S. Bhaskar, Commissioner and Secy, Health and Family welfare, Govt. of Assam	Member
5	Shri Ashutosh Dixit, JS Dept. of Revenue	Member
6	Prof. Bharat Bhaskar, IIM Lucknow	Member
10	Shri Ram Sewak Sharma, DG UIDAI	UIDAI Rep.
11	Shri Srikanth Nadhamuni	UIDAI Rep.
12	Dr. Pramod K. Varma	UIDAI Rep.

Sd/-

(N. Vittal)

Chairman, DDSVP Committee

ANNEXURE-P8

Sl. NO	Bank Name
1	Abhyudaya Co-operative Bank
2	Allahabad Bank
3	Allahabad UP Gramin Bank
4	Andhra Bank
5	The Andhra Pradesh state cooperative Bank Ltd
6	Andhra Pragathi Grameena Bank
7	AP Mahesh Cooperative Bank
8	Apna Sahakari Bank Ltd.
9	Assam Gramin Vikash Bank
10	Axis Bank
11	Bangiya Gramin Vikash Bank
12	Bank of Bahrain & Kuwait
13	Bank of Baroda
14	Bank Of India
15	Bank of Maharashtra
16	BARODA GUJARAT GRAMIN BANK
17	Baroda Rajasthan Kshetriya Gramin Bank
18	BARODA UTTAR PRADESH GRAMIN BANK
19	Bassein Catholic Co-Op Bank Ltd
20	Bihar Gramin Bank
21	Canara Bank
22	Capital Local Area Bank
23	Central Bank of India
24	CENTRAL MADHYA PRADESH GRAMIN BANK
25	Chaitanya Godavari Grameena Bank
26	CITIBANK N A
27	City Union Bank Limited
28	Corporation Bank
29	DECCAN GRAMEENA BANK
30	Dena Bank
31	Dena Gujarat Gramin Bank
32	DEVELOPMENT BANK OF SINGAPORE
33	DCB Bank Ltd
34	Dhanalaxmi Bank
35	Dombivili Nagari Sahakari Bank Ltd.
36	Durg Rajnandgaon Gramin Bank
37	Federal Bank
38	Gopinath Patil Parsik Janata Sahakari Bank
39	Gurgaon Gramin Bank
40	Haryana Gramin Bank
41	HDFC Bank Ltd
42	Himachal Gramin Bank
43	ICICI Bank Ltd
44	IDBI Bank
45	Indian Bank
46	Indian Overseas Bank
47	Indusind Bank
48	ING Vysya Bank Ltd
49	Janakalyan Sahakari Bank
50	Janata Sahakari Bank Ltd.

51	JHARKAND GRAMIN BANK
52	Kallappanna Awade Ichalkaranji JanataSahakari Bank
53	Karnataka Bank Ltd.,
54	Karnataka Vikas Grameena Bank
55	Karur Vysa Bank
56	Kashi Gomti Samyut Gramin Bank
57	Kaveri Grameena Bank
58	Kotak Mahindra Bank Ltd
59	Madya Bihar Gramin Bank
60	MAHARASHTRA GRAMIN BANK
61	Malwa Gramin Bank
62	MANIPUR RURAL BANK
63	MEWAR AANCHALIK GRAMIN BANK
64	Mumbai District Central Co-op Bank Ltd
65	Narmada Jhabua Gramin Bank
66	NKGSB CO-Op. Bank Ltd.
67	North Malabar Gramin Bank
68	Nutan Nagarik Sahakari Bank Ltd
69	Oriental Bank of Commerce
70	Pallavan Grama Bank
71	Paschim Banga Gramin Bank
72	Pragathi Gramin Bank
73	Prathama Bank
74	Puduvai Bharathiar Grama Bank
75	Punjab & Maharashtra Co-operative Bank
76	Punjab & Sind Bank
77	Punjab Gramin Bank
78	Punjab National Bank
79	RAJGURUNAGAR SAHAKARI BANK LTD
80	Ratnakar Bank
81	Saptagiri Grameena Bank
82	Saraswat Bank
83	Sarva UP Gramin Bank
84	Shreyas Gramin Bank
85	Sindhudurg District Central Cooperative Bank Ltd
86	South Indian Bank
87	South Malabar Gramen Bank
88	Standard Chartered Bank
89	State Bank of Bikaner & Jaipur
90	State Bank of Hyderabad
91	State Bank of India
92	State Bank of Mauritus Ltd.
93	State Bank of Mysore
94	State Bank of Patiala
95	State Bank of Travancore
96	SUTLEJ GRAMIN BANK
97	Syndicate bank
98	Tamilnad Mercantile Bank Ltd.
99	Thane Bharat Sahakari Bank Ltd.
100	Thane Janata Sahakari Bank
101	THE ABHINAV SAHAKARI BANK LIMITED

102	THE AHMEDABAD MERCANTILE CO-OP BANK LTD
103	THE ARYAPURAM COOPERATIVE URBAN BANK LTD
104	THE BHARAT CO-OPERATIVE BANK(Mumbai) LTD
105	THE BICHOLIM URBAN CO-OPERATIVE BANK LTD
106	The Catholic Syrian Bank
107	The Citizen Cooperative Bank Limited
108	The Commercial Cooperative Bank Limited
109	THE COSMOS CO-OPERATIVE BANK LTD
110	THE GAYATRI COOPERATIVE URBAN BANK LTD
111	THE GOA STATE CO-OPERATIVE BANK LTD
112	The Goa Urban Co-Operative Bank Ltd.
113	The Greater Bombay Co-operative Bank Limited
114	The Himachal Pradesh State Co-operative Bank Ltd
115	The Jammu And Kashmir Bank Ltd
116	The Kalupur Commercial Co-Operative Bank
117	The Kalyan Janata Sahakari Bank Ltd.
118	THE KANGRA CENTRAL CO-OPERATIVE BANK LTD
119	The Kapol Co-Operative Bank Ltd.
120	The Karad urban Co-op Bank Ltd
121	The Lakshmi Vilas Bank Ltd.
122	The Mahanagar Co-Op. Bank Ltd.
123	THE MAPUSA URBAN COOPERATIVE BANK OF GOA LTD
124	The Mehsana Urban Co-operative Bank
125	THE MUNICIPAL CO-OP BANK LTD
126	The Nasik Merchants Cooperative Bank Ltd
127	The Pochampally Cooperative Urban Bank Ltd
128	The Sahebrao Deshmukh Co-Op. Bank Ltd.
129	The Shamrao Vital Co-operative Bank
130	The Thane Dist. Central Co-op. Bank Ltd
131	Tripura Gramin Bank
132	UCO Bank
133	Union Bank of India
134	United Bank of India
135	UTTAR BIHAR GRAMIN BANK
136	VASAI VIKAS SAHAKARI BANK LTD
137	Vijaya Bank
138	WAINGANGA KRISHNA GRAMIN BANK
139	YES Bank
140	THE GADCHIROLI DISTRICT CENTRAL COOPERATIVE BANK
141	The Adarsh Cooperative Urban Bank Limited
142	THE JALGAON PEOPLES CO OP BANK LTD
143	Ahmednagar Shahar Sahakari Bank Maryadit
144	UTTARBANGA KSHETRIYA GRAMIN BANK
145	The Akola District Central Cooperative Bank Ltd
146	JALGAON JANATA SAHKARI BANK LTD
147	THE CHIPLUN URBAN COOPERATIVE BANK LTD
148	VIVEKANAND NAGRIK SAHKARI BANK MYDT
149	The Vishweshwar Sahakari Bank Ltd
150	SMRITI NAGRIK SAHAKARI BANK
151	The Kolhapur Urban Co-op Bank Ltd
152	The Baghat Urban Co-op Bank Ltd

200

153	MAHAVEER CO-OPERATIVE URBAN BANK LIMITED
154	Marudhara Gramin Bank
155	YADAGIRI LAKSHMI NARSIMHA SWAMY Coop Urban Bank
156	ANDHRA PRADESH GRAMEENA VIKAS BANK
157	Thrissur District Cooperative Bank Ltd
158	THE HASTI CO-OP. BANK LTD.
159	Raigad District Central Co-op Bank Ltd
160	The Madgaum Urban Cooperative Bank Ltd
161	THE HINDUSTHAN CO-OPERATIVE BANK LTD
162	THE PACHORA PEOPLES CO-OP. BANK LTD.PACHORA
163	THE PUNJAB STATE COOPERATIVE BANK LTD
164	Nagpur Nagarik Sahakari Bank Ltd.
165	THE ERNAKULAM DISTRICT CO-OPERATIVE BANK LTD
166	The Ajara Urban Co-op. Bank Ltd.
167	THE SATARA DISTRICT CENTRAL CO-OPERATIVE BANK LTD.
168	AMBARNATH JAI-HIND CO-OP.BANK LTD.
169	TIRUPATI URBAN CO-OP. BANK LTD.
170	Kolhapur Mahila Sahakari Bank Ltd.
171	THE CHANDIGARH STATE CO-OP BANK LTD
172	The West Bengal State Co-op Bank Ltd
173	THE KARAD JANATA SAHAKARI BANK LTD
174	UNIVERSAL CO-OPERATIVE URBAN BANK LTD.
175	Adarniya P.D. Patilsaheb Sahakari Bank Ltd.
176	THE NAWANSHAHR CENTRAL COOPERATIVE BANK LTD.
177	THE LUDHIANA CENTRAL COOPERATIVE BANK LTD
178	The Modern Co-op. Bank Ltd.
179	POORNAWADI NAGRIK SAHAKARI BANK M.BEED.
180	THE FARIDKOT CENTRAL CO-OPERATIVE BANK LTD.
181	PRIYADARSHANI NAGARI SAHAKARI BANK LTD., JALNA.
182	THE JALANDHAR CENTRAL COOPERATIVE BANK LIMITED
183	THE FAZILKA CENTRAL COOP. BANK LTD
184	The S.A.S Nagar Central Cooperative Bank Ltd.
185	Rajkot Nagarik Sahakari Bank Ltd.
186	The Bhavana Rishi Coop. Urban Bank Limited
187	Sant Sopankaka Sahakari Bank Ltd.
188	SHREE PANCHGANGA NAGARI SAHAKARI BANK LTD
189	Vishwas Co-op Bank Ltd.
190	Mansing Co-operative Bank Ltd.
191	The Muktsar Central Co-operated Bank Ltd
192	The Ferozepur Central Coop. Bank Ltd
193	NAVANAGARA URBAN CO-OPERATIVE BANK LTD.
194	VARDHAMAN (MAHILA) CO-OP. URBAN BANK LTD.
195	Rajarshi Shahu Sahakari Bank Ltd
196	Navabharat Co-op. Urban Bank Ltd.
197	Shri Veershaiv Co-op Bank Ltd.
198	The Baramati Sahakari Bank Ltd
199	The Bhagyalakshmi Mahila Sahakari Bank Ltd
200	Pandyan Grama Bank
201	The Gurdaspur Central Cooperative Bank Ltd
202	Deendayal Nagari Sahakari Bank Ltd
203	THE MOGA CENTRAL COOPERATIVE BANK LTD

204	Shivdaulat Sahakari Bank Ltd.
205	PUSAD URBAN CO-OP,BANK LTD.
206	Sangli Urban Co-operative Bank Ltd
207	Janseva Nagari Sahakari Bank Marydit
208	The Haryana State Co-operative Apex Bank Ltd.
209	THE RAJASTHAN STATE CO-OPERATIVE BANK LTD
210	SHRI ADINATH CO-OP.BANK LTD.
211	The Malkapur Urban Co-op Bank Ltd
212	MALDA DISTRICT CENTRAL COOPERATIVE BANK LTD
213	JANATA CO-OP. BANK LTD.
214	Yeshwant Nagari Sahakari Bank Ltd
215	Pune District Central Co-operative Bank Ltd.
216	Janaseva Sahakari Bank Ltd.,Pune
217	JALNA MERCHANTS CO-OP BANK LTD.
218	The Bathinda Central Co-operative Bank Ltd.
219	The Tarn Taran Central Cooperative Bank Ltd
220	SANGLI DISTRICT CENTRAL CO-OP BANK LTD
221	BEAWAR URBAN CO-OPERATIVE BANK LTD.
222	THE CO-OPERATIVE BANK OF RAJKOT LTD
223	The Patiala Central Cooperative Bank Ltd.
224	The Citizens Urban Cooperative Bank Ltd.
225	SUVARNAYUG SAHAKARI BANK LTD.
226	The Sangrur Central Co-operative Bank Ltd.
227	The Bhadgaon People's Co-op Bank Ltd.
228	Bhagini Nivedita Sahakari Bank Ltd.
229	Shree Mahalaxmi Urban Co-op Credit Bank Ltd.
230	The Chembur Nagarik Sahakari Bank
231	THE SEVA VIKAS CO-OP.BANK LTD.
232	Shivajirao Bhosale Sahakari Bank Ltd
233	The Hoshiarpur Central Co-operative Bank Ltd
234	The Ropar Central Cooperative Bank
235	THE SONEPAT URBAN CO-OP.BANK LTD.
236	THE FATEHGRAH SAHIB CENTRAL COOPERATIVE BANK
237	PEOPLES' CO-OPERATIVE BANK LTD,Hingoli
238	The District Co-Operative Central Bank Ltd.Medak
239	THE NALGONDA DIST. CO-OP. CENTRAL BANK LTD.
240	The Warangal District Cooperative Central Bank Ltd
241	The Kapurthala Central Cooperative Bank Ltd
242	Sharad Sahakari Bank Ltd
243	The Guntur District Cooperative Central Bank Ltd.
244	The District Cooperative Central Bank Ltd, Kurnool
245	The Krishna District Cooperative Bank
246	Annasaheb Chougule Urban Co-op Bank Ltd.
247	Solapur Janata Sahakari Bank Ltd.
248	SHREE WARANA SAHAKARI BANK LTD.
249	Jodhpur Nagrik Sahakari Bank Limited
250	Raigad Sahakari Bank Limited
251	The Hyderabad District Cooperative Bank Ltd
252	The Adilabad District Co-Op Central Bank Ltd.
253	The Anantapur District Cooperative Central Bank Lt
254	The District Cooperative Central Bank,Mahabubnagar

255	SRI POTTI SRIRAMULU NELLORE DCCB
256	The District Cooperative Central Bank Ltd,Srikakul
257	The Panipat Urban Cooperative Bank Ltd
258	THE CHIKHLI URBAN CO-OP BANK LTD.
259	The Washim Urban Co-operative Bank Ltd.
260	The Amritsar Central Cooperative Bank Limited.
261	SHIVALIK MERCANTILE CO-OP BANK Ltd
262	The Union Co-operative Bank Ltd
263	Sudha Co-operative Urban Bank Ltd
264	The District Coop Central Bank Ltd,Vizianagaram
265	The Karimnagar District Cooperative Central Bank
266	The District Co-op Central Bank Ltd, Kakinada
267	SHRI CHHATRAPATI RAJARSHI SHAHU URBAN CO-OP BANK
268	The Chittoor District Co-op Central Bank Ltd
269	The Prakasam District Co-op Central Bank Ltd
270	The Annasaheb Savant Co-op Urban Bank Mahad Ltd
271	The Nizamabad District Co-op Central Bank Ltd
272	Shri Mahavir Urban Co-operative Bank Ltd
273	The Agrasen Co-operative Urban Bank Ltd
274	The NAV Jeevan Co-op Bank Ltd
275	The Kadappa District Co-operative Central Bank Ltd
276	The District Central Coopearative Bank Ltd,Khammam
277	The District Central Coop Bank Limited, Elluru
278	SUCO SOUHARDA SAHAKARI BANK
279	Mantha Urban Co op Bank Ltd
280	THE NATIONAL CO-OPERATIVE BANK LTD
281	The Kannur District Co-operative Bank Ltd
282	The District Co-op Central Bank Ltd, Visakhapatnam
283	The Junagadh Commercial co-op bank Ltd
284	THE KARNATAKA STATE CO-OPERATIVE APEX BANK LTD.
285	Yavatmal District Central Co-operative Bank Ltd
286	THE YASHWANT CO-OP BANK LTD
287	Prime Co-Operative Bank Ltd.
288	Jijamata Mahila Sahakari Bank Ltd
289	Parshwanath Co-operative Bank Ltd
290	PRERANA CO-OP BANK LTD.
291	Fingrowth Co-operative Bank Ltd
292	Vasai Janata Sahakari Bank Ltd
293	THE SAHYADRI SAHAKARI BANK LTD
294	The Sultan's Battery Co-operative Urban Bank Ltd
295	The Udaipur Mahila Urban Co-op Bank Ltd
296	Tamluk Ghatal Central Coop Bank
297	Guardian Souharda Sahakari Bank Niyamita
298	Adarsh Co-operative Bank Ltd
299	PATAN CO-OPEARTIVE BANK LTD
300	KOKAN MERCANTILE CO-OPERATIVE BANK LTD

203

ANNEXURE:P-7 (Colly)

ITEM NO.1 COURT NO.4 SECTION PIL

SUPREMECOURTOFINDIA
RECORD OF PROCEEDINGS

WRIT PETITION (CIVIL) NO. 196 OF 2001

PEOPLE'S UNION FOR CIVIL LIBERTIES ..Petitioner(s)

VERSUS

UNION OF INDIA & ORS. ..Respondent(s)

(Regarding reports submitted by Justice D.P. Wadhwa, Retd. Judge, Supreme Court of India) (REG. PUBLIC DISTRIBUTION SYSTEM)

I.A. Nos.90, 93, 98, 102 to 108, 110, 111 & 112 in W.P.(C) No.196/2001

(For permission on behalf of Respondent No.17 i.e. State of Maharashtra, modification and directions, intervention on behalf of West Bengal M.R. Dealers Association and All Bengal Price Shop Dealers Welfare Association, impleadment, exemption from filing O.T., directions,extension of time on behalf of State of Rajasthan, modification of Court's order dt.22.04.2009,

impleadment on behalf of Karnataka State Taluka Co-operative Marketing Society Association to be impleaded as respondents and permission to file additional affidavit)

WITH
CONTEMPT PETITION (CIVIL) NO. 99/2009
(With Application for exemption from filing O.T.)

W.P.(C) No. 277/2010

Date:14/09/2011 These Petitions were called on for hearing today.

CORAM :
HON'BLE MR. JUSTICE DALVEER BHANDARI
HON'BLE MR. JUSTICE DEEPAK VERMA

For Petitioner(s) Mr. Colin Gonsalves,Sr.Adv.
Mr. Divya Jyoti,Adv.
Ms. Jyoti Mendiratta,Adv.

For Respondent(s) Mr. Mohan Parasaran,ASG
Mr. D.L. Chidananda,Adv.
Mr. S. Wasim A. Qadri,Adv.
Mr. A. Dev Kumar,Adv.
Ms. Sunita Sharma,Adv.
Ms. Sushma Suri,Adv.
Ms. Anil Katiyar,Adv.
Ms. Supriya Jain,Adv.
Mr. D.S. Mahra,Adv.
Mr. Sudarshan Singh Rawat,Adv.

For DDA Mr. Vishnu B. Saharya,Adv.
For M/s. Saharya & Co.,Advs.

Mr. Jana Kalyan Das,Adv.

Mr. Ranjan Mukherjee,Adv.
Mr. S.C. Ghosh,Adv.

Ms. Hemantika Wahi,Adv.
Ms. Suveni Banerjee,Adv.

Mr. D.K. Goswami,Adv.
Mr. Shirish Kr. Mishra,Adv.

Mr. Pragyan P. Sharma,Adv.
Mr. Siddhartha Lodha,Adv.
for Mr. P.V. Yogeswaran,Adv.

Mr. H.P. Raval,ASG
Ms. Indra Sawhney,Adv.

Dr. Manish Singhvi,AAG,Raj.
Mr. Devanshu Kumar Devesh,Adv.
Mr. Irshad Ahmad,Adv.
Mr. Milind Kumar,Adv.

Mr. A. Mariarputham,Adv.Gen,
Mrs. Aruna Mathur,Adv.
Mr. Avneesh Arputham,Adv.
Mr. Yusuf Khan,Adv.
For M/s. Arputham Aruna & Co.,Advs.

Mr. Riku Sarma,Adv.
Mr. Navnit Kumar,Adv.
for M/s. Corporate Law Group,Advs.

Ms. Rachana Srivastava,Adv.
Mr. Ranchi Daga,Adv.
Mr. Krutin Joshi,Adv.

Mr. Manoj Saxena,Adv.
Mr. Mayank Nigam,Adv.
Mr. T.V. George,Adv.

Ms. Kamini Jaiswal,Adv.

Mr. Shish Pal Laler,Adv.

Mr. Khwairakpam Nobin Singh,Adv.
Mr. Sapam Biswajit Meitei,Adv.

Mr. Ranjan Mukherjee,Adv.

Mr. Jatinder Kumar Bhatia,Adv.

Mr. R. Sundaravaradhan,Sr.Adv.
Mr. V.G. Pragasam,Adv.
Mr. S.J. Aristotle,Adv.
Mr. Prabu Ramasubramanian,Adv.

Mr. G.V. Rao,Adv.
Mr. Ravi Prakash Mehrotra,Adv.

Mr. Gopal Singh,Adv.
Mr. Manish Kumar,Adv.
Mr. Chandan Kumar,Adv.

Mr. Bikas Kar Gutpa,Adv.
Mr. Abhijit Sengupta,Adv.

Mr, Rituraj Biswas,Adv.

Mr. Manish Pitale,Adv.
Mr. Wasi Haider,Adv.

For Mr. C.S. Ashri,Adv.

Mr. Soumitra G. Chaudhuri,Adv.
Mr. Tara Chandra Sharma,Adv.

Mr. Anil Shrivastav,Adv.
Mr. Ritu Raj Biswas,Adv.

Mr. Edward Belho,Adv.
Mr. P. Athuimei R. Naga,Adv.
Mr. K. Enatoli Sema,Adv.
Mr. Nimshim Vashum,Adv.

Mr. T. Harish Kumar,Adv.
Mr. V. Vasudevan,Adv.

Mr. Sanjiv Sen,Adv.
Mr. Prashant Kumar,Adv.
Mr. P. Parmeswaran,Adv.
Mr. Ujjal Banerjee,Adv.

Mr. Atul Jha,Adv.
Mr. D.K. Sinha,Adv.

Mr. G.V. Chandrashekhar,Adv.
Mr. N.K. Verma,Adv.
Ms. Anjana Chandrashekar,Adv.

Mr. Gopal Prasad,Adv.
Mr. Sarbojit Dutta,Adv.

Mr. D. Mahesh Babu,Adv.
Mr. Ramesh Allanki,Adv.
Mr. Savita Dhande,Adv.
Mr. V. Pattabhi,Adv.

Mr. Sunil Fernandes,Adv.

Mr. Suhaas Joshi,Adv.
Ms. Astha Sharma,Adv.

Mr. Ramesh Babu M.R.,Adv.

Ms. Anuradha Rustagi,Adv.
Ms. D. Bharathi Reddy,Adv.

Mr. Sanjay R. Hegde,Adv.
Mr. Ramesh Kr. Mishra,Adv.

Ms. Sumita Hazarika,Adv.

Mr. K.K. Mahalik,Adv.
Mr. Ajay Pal,Adv.

Mr. Manjit Singh,Adv.
Mr. Kamal Mohan Gupta,Adv.

Ms. A. Subhashini,Adv.

Mr. Gopal Singh,Adv.
Mr. Rituraj Biswas,Adv.

Mr. Kuldip Singh,Adv.
Mr. R.K. Pandey,Adv.
Mr. H.S. Sandhu,Adv.
Mr. K.K. Pandey,Adv.
Mr. Mohit Mudgil,Adv.

Mr. Ravindra Keshavrao Adsure,Adv.

Ms. Bina Madhavan,Adv.

Mr. Prashant Kumar,Adv.

Mr. Vishwajit Singh,Adv.

Mr. Sanjay V. Kharde,Adv.
Ms. Asha G. Nair,Adv.

Mr. K.V. Mohan,Adv.

Mr. Rajesh Srivastava,Adv.

Mrs. Promila,Adv.
Mr. S. Thananjayan,Adv.

Mr. Anuvrat Sharma,Adv.

Mr. K.N. Madhusoodhanan,Adv.
Mr. R. Sathish,Adv.

Mr. Naushad Ahmad Khan,Adv.
Mr. Rajesh Kumar Verma,Adv.
for Mr. R.C. Kaushik,Adv.

Mr. Pradeep Misra,Adv.

Mr. Venkateswara Rao Anumolu,Adv.

Mr. Bikas Upadhyay,Adv.
Mr. B.S. Banthia,Adv.

Dr. Aman Hingorani,Adv.
Ms. Priya Hingorani,Adv.

Mr. G. Prakash,Adv.
Ms. Beena Prakash,Adv.
Mr. V. Senthil,Adv.

Mr. Navneet Kumar,Adv.

Mr. Anil Kumar Jha,Adv.

Mr. Vikas Mehta,Adv.

Mr. Pramod Swaroop,Sr.Adv.
Mr. Raj Kumar Gupta,Adv.
Mr. Rajiv Dubey,Adv.
Mr. Kamlendra Mishra,Adv.
6

Mr. Naresh K. Sharma,Adv.

Mr. Anis Suhrawardy,Adv.

Mr. Shivaji M. Jadhav,Adv.

Mr. Suresh Chandra Tripathy,Adv.

Mr. Navin R. Nath,Adv.

UPON hearing counsel the Court made the following

ORDER

The High Powered committee headed by Justice D.P. Wadhwa, Retired Judge of this Court, has submitted a Preliminary Report on Computerization of Public Distribution System. In the recommendations of the Report it is mentioned that Computerization of PDS consists of primarily three components i.e. creating a updating beneficiary database, stocks management from FCI till FPS and sale of commodities at Fair Price Shops. In order to make PDS effective it is important that the delivery and management system is

transparent. The citizen participation for social audit can play a crucial role in ensuring effectiveness of the system. In order to implement this system across the country, the following actions are suggested by the Committee:

1. End to end computerization of PDS may be considered in two parts and following prioritisation of the Implementation Strategy may be followed:

Component I:- Diversions, leakages, delays in allocation and transportation, inappropriate distribution of foodgrains to fair price shops go unchecked because of lack of visibility of this information in the public domain.

Computerization of complete supply chain management up to the shop level and availability of this information on a Transparency Portal in public domain is to be accorded the highest priority. The portal should have different dashboards catering to the information needs of all the stakeholders.

Component II:- Electronic authentication of delivery and payments at the fair price shop level. In order to ensure that each card holder is getting his due

entitlement computerization has to reach literally every doorstep and this could take long. Moreover several States have already started implementing smart cards, food coupons etc. which have not been entirely successful.

Reengineering these legacy systems and replacing it with online Aadhaar authentication at the time of foodgrain delivery will take time. This is therefore proposed as component II.

2. Department of Food & Public Distribution is directed to immediately issue guidelines to all the States for end to end computerization of TPDS.

3. Government of India shall ensure that State Governments prepare a time bound action plan for completing the process of computerization. These action plan will be implemented keeping the timelines in mind and will be regularly submitted before the Hon'ble Supreme Court.

4. States/UTs should take up End to End computerization of TPDS as a top priority and should

appoint a dedicated nodal officer to monitor the projects related to TPDS computerization.

5. States/UTs maybe encouraged to include the PDS related KYR+ field in the date collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhaar) enrolment.

6. Digitization of beneficiary data and a centralized database with clear process of data updation to be put in place by States in a time bound manner.

7. Dissemination of information about availability of foodgrains through SMS to the pre-identified individuals in the local community to enable social audit. The system could also provide stock position at a specific location on demand. The information related to stock availability using latest technological inter face should be made available in a public domain.

8. Single unified information system should be developed to meet the above mentioned requirements that would help to achieve certain basic level of

transparency in PDS. For this states should arrange training programs for field functionaries and FP dealers.

9. Chhattisgarh model of computerization for PDS System, (A note on the computerization of PDS in the State of Chhattisgarh is annexed hereto as Annexure II) which primarily cater to the computerization upto the shop level was also deliberated upon and discussed in the HPC. It was decided that the Chhattisgarh model may be adopted for component 1 and component 2 maybe done on the similar lines of the Gujarat model of computerization.

The Chhattisgarh model may be implemented in all the States within a maximum period of three months. However, some State Governments like Government of Gujarat which is following Component 2, or other States which may be at the advanced stage of following some other model, such States may continue to follow the same so long as it is fulfilling the end objectives of completing the computerization. (A note on the computerization of PDS in the State of Gujarat is annexed hereto as Annexure III).

10. As the process of end to end computerization is expected to be a sizable exercise, to complete it in a mission mode, a separate and dedicated institutional mechanism is to be incorporated to look after the progress of computerization of PDS. This institution must have active participation of all stake holders including the State Governments. As PDS is implemented by the State by the State Governments and supported by Government of India, role of State Government in this body will be helpful in getting required support from the State Governments.

11. Information related to stock availability, movement and date quantity of stocks supplied to FPS should be made available in public domain by using latest technological interface like SMSs/website or other means.

12. As far as possible, state governments should be directed to link the process of computerization of Component-2 with AADHAR Registration. This will help in streamlining the process of biometric collection as well as authentication. States/UTs may be encouraged to include the PDS related KYR+ field in the data

collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhar) enrolment.

13. An effective grievance redressal mechanism should be strictly enforced based on SMS/email and other suitable technology. Government of India should ensure that this mechanism is put in place in all the states. State/UTs should create effective grievance redressal mechanism where use of mobile based SMS/email can be used for timely resolution of the citizen/beneficiary grievance. A four digit toll free number may be established in all the States for grievances registration and redressal thereof.

14. Government of India will ensure that the computerization operation is provided necessary infrastructure and financial support. This needs to be completed in a time bound manner and the institution mechanism so created shall be completely responsible for meeting the timelines. Government of India with the help of state government will ensure that the institution

has sufficient infrastructure and finances to complete the computerization in a time bound manner.

15. While this complete process is expected to take some time, in the meantime, following action may immediately be taken.

a. State Governments will ensure door step delivery of food grain for the ration shops in a time bound manner and shall ensure that information related to movement and availability of food grain is available in public domain.

b. A PDS Public Information portal may be made which will have information related to complete public distribution system. In addition to other information, it should also have the information of date and quantity of food grain supplied to the fair price shop every month for all the shops.

c. The digitized database of ration cards will be put up in the public domain including on the websites.

d. State should make necessary amendments to make the fair price shop financially viable.

e. A four digit toll free number may be established in all the States for grievances registration and redressal thereof.

f. All the State governments will ensure that required allocation reaches the fair price shop before 1st day of the month and this information should be available on the transparency portal.

g. A drive can be started to eliminate the fake and ghost ration cards. A comparison with data available with other departments like election, census etc. gives the quick estimates about the bogus cards. It was seen that at some places, units in the ration cards exceed even the populations of the area. These practices should be checked immediately. This can also be linked up with the Socio Economic Census in Rural Areas which is expected to be completed shortly within this year itself.

h. Government of India shall ensure that all the state governments prepares a time bound action plan for complete computerization of PDS system within three months' time. Strict deadlines may be fixed in the action plan and these will be submitted before Hon'ble Supreme Court within three months period.

i. All above steps may be completed within three months time.

We have discussed the recommendations of the High Powered Committee on Computerization with the learned counsel for the petitioner and the learned Additional Solicitor General of India. The Government of India has agreed in principle to implement these recommendations as expeditiously as possible. We request Mr. Parasaran, learned Additional Solicitor General to ensure that the process of computerization is completed as expeditiously as possible. He may help in coordinating with the High Powered Committee and other concerned authorities and individuals.

We direct the Chief Secretaries of various States to indicate, within two weeks, as to how much

additional foodgrains is required for the poorest districts in their States and allocation of foodgrains would be made within two weeks thereafter. We further direct the Chief Secretaries to ensure that whatever foodgrains are allocated, the same be lifted by them within two weeks thereafter. The allocation of goodgrains to be made out of five million tonnes additionally allocated.

We request the High Powered Committee to hear all the parties and decide whether the foodgrains is required to be distributed at AAY rates or BPL rates and the decision of the High Powered Committee would be binding on all concerned and would be implemented forthwith.

We request the High Powered Committee to decide this issue as expeditiously as possible and we direct the parties to appear before the High Powered Committee on 20th September, 2011. In case the Chief Secretaries of various States do not respond within two weeks, as directed above, it would be presumed that, that particular State does not require additional foodgrains at AAY or BPL rates.

222

Reportable

IN THE SUPREME COURT OF INDIA
[CIVIL APPELLATE JURISDICTION]

CIVIL APPEAL NO. 958 OF 2013
(Arising out of SLP(C) No.9162 of 2011)

State of Kerala and others ..... Appellants

Versus

President, Parent Teacher Assn. SNVUP
and others ... Respondents

JUDGMENT

K.S. Radhakrishnan, J.

1. Leave granted.

2. We are in this appeal concerned with the question whether the High Court was justified in directing the Secretary, General Education Department of the State of Kerala to get the verification of the actual students' strength in all the aided schools in the State with the assistance of the police and to take appropriate action.

3. The Assistant Educational Officer (AEO), Valappad had fixed the staff strength of S.N.V.U.P. School, Thalikulam for the year 2008-09 based on the

visit report of High School Association (SS), GHS Kodakara as per Rule 12 of Chapter XXIII of Kerala Education Rules (KER). Later, based on a complaint regarding bogus admissions and irregular fixation of staff for the year 2008-09 by the AEO, the Super Check Cell, Malabar Region, Kozhikode made a surprise visit in the school on 17.09.2008 and physically verified the strength of the students and noticed undue shortage of attendance on that day. The strength verified by the Super Check Cell was not sufficient for allowing the divisions and posts sanctioned by the AEO. The Head Master of the School, however, stated in writing that the shortfall of attendance on the day of inspection was due to "Badar Day" of Muslim community and due to distribution of rice consequent to that. In order to confirm the genuineness of the facts stated by the Head Master, the Cell again visited the school on 16.12.2008. Verification could not be done on that day, hence the Cell again visited the school on 02.02.2009 and physically verified the students' strength. On that day also, there were large number of absentees as noticed on 17.09.2008. On verification of attendance

register, it was found that the class teachers of respective classes had given bogus presence to all students on almost all the days. Enquiry revealed that the school authorities had obtained the staff fixation order for the year 2008-09 through bogus recordical admissions.

4. The Director of Public Instructions (DPI), Thiruvananthapuram consequently issued a notice dated 07.05.2009 to the Manager of the School of his proposal to revise roll strength and revision of staff strength by reducing one division each in Std. I, II, IV to VII and 2 divisions in Std. III and consequent posts of 5 LPSAs, 3 UPSAs in the school during the year 2008-09. The Manager of the school responded to the notice vide representation dated 27.05.2009 stating that Super Check Officials did not record the attendance particulars of the students in the visit record and had tampered with the attendance register. The Manager had also pointed out that the Headmaster was not responsible to compensate the loss suffered by the Department by way of paying salary to the teachers who had worked in the sanctioned posts. Further, it

was also pointed out that the staff fixation should not be done within the academic year and re-fixation was not permissible as per Rule 12E(3) read with Rule 16 of Chapter XXIII, KER and requested not to reduce the class divisions.

5. The DPI elaborately heard the lawyers appearing for the Headmaster and the Manager of the school, affected teachers as well as the officials of the Super Check Cell. Having heard the submissions made and perusing the records made available, the DPI found that the staff fixation of the school for the year 2008-09 was obtained through bogus admissions and misrepresentation of facts. DPI noticed that the roll strength during the year 2008-09 was 1196. There were 404 absentees on the first visit of the Cell on 17.09.2008. The Super Check Cell again visited the school on 16.12.2008 and 02.02.2009 and it was found that among 404 students absent on the first day, 179 names were bogus and irregular retentions. The physical presence of 179 students could not be verified on all the three occasions. DPI, therefore, passed an order revising the staff fixation of the school for the

year 2008-09 as per Rule 12(3) read with Rule 16 of Chapter XXIII of KER. Consequently, the total number of divisions in the school was reduced to 23 from 31. In the Order dated 08.09.2009, the DIP had stated as follows:

> "The Headmaster is responsible for the admission, removals, and maintenance of records and for the supervision of work of subordinates. It is the duty of the verification officer to verify the strength correctly and to unearth the irregularities. Due to the irregular fixation of staff, the State exchequer has incurred additional and unnecessary expenditure by way of pay and allowances for 8 teachers and expenditure incurred in connection with payment of various scholarships, lump-sum grant, noon-feeding, free books etc to the bogus students. These loss sustained to the Government will be recovered from the

Headmaster of the school who alone is responsible for all the above irregularities."

6. The DPI also directed to take further action to fix the liabilities and recover the amount from the Headmaster under intimation to DPI and the Super Check Officer, Kozhikode. The Headmaster and Manager of the school, aggrieved by the above-mentioned order, filed a revision petition before the State Government. The High Court vide its judgment dated 7.12.2009 in Writ Petition (C) No. 35135 of 2009 directed the State Government to dispose of the revision petition.

7. The higher level verification was also conducted in the school with regard to the staff fixation for the year 2009-10 and on verification, it was found that many of the students in the school records were only bogus recordical admissions. Following that, the AEO issued staff fixation order for the year 2009-10 vide proceedings dated 27.03.2010.

8. Meanwhile, the President of the Parent Teachers Association (Respondent No.1 herein) filed WP (C) No.

12285 of 2010 before the High Court seeking a direction to the AEO to reckon the entire students present in the school on the 6th working day and higher level verification of District Education Officer (DEO) on 13.01.2010 for the purpose of staff fixation for the year 2009-10 and also for a declaration that the exclusion of the students who were present on the day of higher level verification on 13.01.2010 from the staff fixation order 2009-10 was illegal and also for other consequential reliefs.

9. Learned Single Judge of the High Court dismissed the Writ Petition on 07.04.2010 stating that the Parent Teachers Association have no locus standi in challenging the staff fixation order. The judgment was challenged in W.A No.1195 of 2010 by the President, Parent Teachers Association before the Division Bench of the High Court and the Bench passed an interim order on 14.07.2010. The operative portion of the same reads as follows:-

> "The inspection team has recorded that as many as 179 students whose names and particulars are furnished, represent bogus admissions for

record purposes. If admission register is manipulated by recording bogus admissions in the name of non- existing students or students of other institutions, we fell criminal action also is called for against the school authorities. Since appellant has denied the findings in the inspection report, we fell a police enquiry is called for the in the matter. We, therefore, direct the Superintendent of Police, Thrissur to constitute a team of Police Officers to go through Ext.P1, verify the registered maintained by the school authorities, take the addresses as shown in the school records and conduct field enquiry as to whether the students are real persons and if so, whether they are really studying in this school or elsewhere. In other words, the result of the enquiry is to confirm to this court whether the students whose names are in the record of the school are real and if so, whether they are students in this school or any other school."

The Bench also directed to the Superintendent of Police to submit his report within one month.

10. The Superintendent of Police, following the direction given by the High Court, constituted a team under the leadership of the Circle Inspector of Police, Valappad and the team conducted detailed enquiry in respect of all the matters directed to be examined by the police. The Superintendent of Police submitted the report dated 20.09.2010 which reads as follows:

> "On the enquiry about the 187 students (179+8) which were alleged as bogus admissions as per Ext.P1, it is revealed that only 72 students were studied in S.N.V.U.P. School during the period 2008- 09 and 80 students were studied in some other schools. The addresses of 23 students have not been traced out even with the help of postman of the concerned area. On the enquiry it is also revealed that 4 students vide the admission Nos. 13008, 11875, 12883 and 13876 mentioned in Ext.P1, have not been studied anywhere during that period.
>
> The details of the 187 students, revealed in the enquiry are mentioned below:-

1.	Actual No. of students studied in SNVUP School, Thalikulam during 2008-2009	72
2.	No. of Students studied in some other schools	80
3.	No. of students whose address have not been trace out	23
4.	No. of students have not been studied anywhere	04
5.	No. of students removed from the rolls. Immediately after strength inspection	08
	Total 187	

The report of the enquiry, submitted by the Circle Inspector of Police, Valappad showing the details of each students is also produced herewith."

11. The Division Bench of the High Court after perusing the report submitted by the Superintendent of Police found that neither the finding of the DPI based on inspections by Super Check Cell nor the claim of the Parent Teachers Association was correct since the police had found that at least 72 out of 187 students

declared bogus by the DPI were real students of the school. The High Court, therefore, concluded manipulation by the school management was obvious, though not to the extent found by the Super Check Cell based on which DPI had passed the impugned order. The Division Bench expressed anguish that the management had included 80 students studying in other schools as students of the present school. It was also noticed that as many as 23 students could not be traced by the police with the help of the postman, were also included in the register.

12. The Division Bench concluded that since the Super Check Cell, the Education Department lacked the investigating skill or the authority to collect information from the field, it would be appropriate that the verification of actual students in all the aided schools in the State would be done through the police. Holding so, the High Court gave the following direction:

> "We, therefore, feel as in this case Police should be entrusted to assist the Education Department by conducting enquiry about the actual and real students studying in every

aided school in the State and pass on the same to the Education Department for them to fix or re-fix the staff strength based on the data furnished by the Police. We, therefore, direct the Secretary, Department of Education, to get verification of the actual students studying in all the aided schools in the State done through the police authorities and take appropriate action. It would be open to the Government to consider photo or finger identification of the students for avoiding manipulation in the school registers. The Government is directed to complete the process by the end of this academic year and file a report in this court."

13. The State of Kerala, aggrieved by the various directions given by the Division Bench, has preferred this appeal. Ms. Liz Mathew, learned counsel appearing for the State of Kerala submitted that the High Court was not justified in giving a direction to the Secretary, Education Department in entrusting the task to State Police for verification of actual students' strength in all

the aided schools, while the enquiry is being conducted by the Education Department. Learned counsel submitted that Kerala Education Act and Rules did not prescribe any mechanism for conducting enquiries by the police at the time of staff fixation. The method to be adopted in the fixation of staff in various schools is prescribed under Chapter XXIII of KER and police have no role. The Rules empower the AEO, the DEO and the Super Check Cell etc. to conduct enquiries but not by the police. Learned counsel also pointed out that the presence of the police personnel in the aided schools in the States would not only cause embarrassment to the students studying in the school but would also cast wrong impression on the minds of the students about the conduct of their Headmaster, teachers and staff of the school.

14. We notice that the State itself had admitted in the petition that there should be a better mechanism to ascertain the number of students in the aided schools which could be done by finger printing or any other modern system so that the students could be properly identified and staff fixation could be done on the basis

of relevant data. We, therefore, directed the State to evolve a better mechanism to overcome situations like the one which has occurred in the school. Fact finding authorities have categorically found that the school authorities had made bogus admissions and made wrong recording of attendance which led to the irregular and illegal fixation of staff strength of the school for the years 2008-09 and 2009-10.

15. An additional affidavit has been filed by the State of Kerala stating that the Government after much thought and deliberations formulated a scientific method to resolve the issue emanating from staff fixation orders every year. The affidavit says that the number of students in the school can be determined through Unique Identification Card (UID) technology and the number of divisions could be arrived at on the basis of revised pupil teacher ratio. Further, it is also pointed out that after implementation of UID as a part of scientific package, the government will remand the matter of identification of bogus admission to the DPI for considering issues afresh after corroborating the findings of Super Check Cell with UID details of the

students. The State has issued a circular No. NEP (3) 66183/2011 dated 12.10.2011 which, according to the State, would take care of such situations happening in various aided schools in the State.

16. We are of the view even though the Division Bench was not justified in directing police intervention, the situation that has unfolded in this case is the one that we get in many aided schools in the State. Many of the aided schools in the State, though not all, obtain staff fixation order through bogus admissions and misrepresentation of facts. Due to the irregular fixation of staff, the State exchequer incurs heavy financial burden by way of pay and allowances. The State has also to expend public money in connection with the payment of various scholarships, lump-sum grant, noon-feeding, free books etc. to the bogus students.

17. A great responsibility is, therefore, cast on the General Education Department to curb such menace which not only burden the State exchequer but also will give a wrong signal to the society at large. The Management and the Headmaster of the school should

be a role model to the young students studying in their schools and if themselves indulge in such bogus admissions and record wrong attendance of students for unlawful gain, how they can imbibe the guidelines of honesty, truth and values in life to the students. We are, however, of the view that the investigation by the police with regard to the verification of the school admission, register etc., particularly with regard to the admissions of the students in the aided schools will give a wrong signal even to the students studying in the school and the presence of the police itself is not conducive to the academic atmosphere of the schools. In such circumstances, we are inclined to set aside the directions given by the Division Bench for police intervention for verification of the students' strength in all the aided schools.

18. We are, however, inclined to give a direction to the Education Department, State of Kerala to forthwith give effect to a circular dated 12.10.2011 to issue UID Card to all the school children and follow the guidelines and directions contained in their circular. Needless to say, the Government can always adopt, in future,

better scientific methods to curb such types of bogus admissions in various aided schools.

19. We, however, find no reason to interfere with the direction given by the DPI to take further action to fix the liabilities for the irregularity committed in the school for the years 2008-09 and 2009-10, for which the appeal is pending before the State Government. The State Government will consider the appeal and take appropriate decision in accordance with law, if it is still pending. Appeal is allowed as above without any order as to costs.

.....J.
(K.S. Radhakrishnan)

.....J.
(Dipak Misra)

New Delhi,
February 6, 2013

//TRUE COPY//

239
ANNEXURE-J&K

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

Role of Biometric Technology in Aadhaar Enrollment

Executive Summary

240

*This report focuses on the biometric technology of the UID project for the purposes of UID enrollment. It goes into the proof of concept **studies conducted in India, analysis of the study results, design** decisions on biometric modes necessary in the Indian context, implementation of client and server side systems for enrollment and finally concludes with the accuracy and performance achieved by the UID biometric system using 8.4crore real enrolments.*

Goal: The goal of the UID project is to assign a unique Identification number to each resident of India. The uniqueness constraint implies that during enrolment stage (creation of Aadhaar) each person will get one and only one Aadhaar number. To ensure that each person gets one and only one Aadhaar number it is necessary that the resident's identity information is captured and matched against every other resident (1:N check) who have previously enrolled - This process is called de-duplication.

Uniqueness & Biometrics: It is not possible to de-duplicate 1.2 billion residents by using demographic fields only (like name, address, age, gender .etc) and moreover identity documents that rely only on demographic fields and personal reference checks are surrogates of identity and are vulnerable to forgery, falsification, theft, loss and other corruptions. In Indian context, biometrics were determined to be the most suitable factors for carrying out de-duplication. Hence it is necessary to enrol all residents along with their biometrics and build a clean database for the purposes of a National Identity system.

Biometric Standards Committee: The UIDAI's Biometric Standards Committee headed by Director General NIC (National Informatics Centre), published a report in December 2009 and advised that a biometric system based only on fingerprint might present challenges in India due to a large number of people engaged in manual labour and urged the UIDAI to consider the use of iris in addition to fingerprints in order to improve inclusiveness and accuracy of the system.

Proof-of-Concept Study (PoC): The UIDAI conducted a Proof-of-Concept study during Mar-June 2010 in predominantly rural areas of Andhra Pradesh, Karnataka and Bihar published a report in December 2010 whose key findings included:

- Iris enrollment took less than a minute to capture and could be captured effectively from people, even from those who were blind.
- Children between 4-15 years could be biometrically enrolled correctly, and could be de-duplicated as accurately as adults.
- The accuracy levels achieved with a combination of fingerprint and iris were more than an order of magnitude (10x) better than using one or the other.

The PoC report concluded that "*The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually.*

multi-modal enrolment was adequate to carry out de-duplication on a much larger scale, with reasonable expectations of extending it to all residents of India"

System Design: Based on the biometrics standards committee report, the PoC report, global learning's and expert opinions the UIDAI made the following design choices:

- Selected three biometric modalities of –10 fingerprints, 2 irises and face.
- Created standard client enrollment software - with quality checks for biometric and demographic data, consistency of capture process and encryption of enrolment data for security/data-protection.
- Built an enrollment server to perform demographic de-duplication, biometric de-duplication and manual adjudication of matches found by the system.
- Used commodity hardware, devices standards, open source software wherever possible, and defined standards and APIs (application programming interface) for interoperability and to avoid vendor-lock-in.

The Enrollment status of the UIDAI project as of Dec 31st 2011

- *36,000 Active enrolment stations*
- *59 Registrars, 83 Enrolment agencies in 32 states and union territories*
- *87,000 Certified enrolment operators*
- *11 - Models of certified biometric devices that are deployed in the field*
- *15 crore – Number of residents enrolled in the field*
- *10.25 crore – Number of Aadhaars generated by UIDAI*
- *10 lakhs/day – Peak enrolment processing rate*
- *100 trillion - Biometric person matches conducted every day to issue 10 lakh Aadhaars*

Biometric Accuracy and Effectiveness: In the last few months there have been media reports with misconceptions about the accuracy and efficacy of the UIDAI's biometric system. **The Parliamentary Standing Committee on Finance** (2011-12) that reviewed the National Identification Authority of India bill has referred to an "expert" who has stated *"it has been*

proven again and again that in the Indian environment, the failure to enrol with fingerprints is as high as 15% due to the prevalence of a huge population dependent on manual labour". These misconceptions have been addressed in the box below:

Biometric Accuracy

As of December 31st 2011, the UIDAI has true and tested statistics computed from real operational large-scale UIDAI system with the resident enrollment database size of 8.4 crore (84 million). It is unnecessary and inaccurate to attempt to infer UIDAI system performance from other systems which are ten to thousand times smaller. Specifically,

- ***Failure to Enroll(FTE) Rate: Zero**. As a policy, every unique resident, regardless of their biometrics can be enrolled and issued Aadhaar number.*
- ***Biometric Failure to Enrol Rate: 0.14%**. This implies that 99.86% of the population can be uniquely identified by the biometric system. The exceptions (0.14%) however are de-duplicated using demographic data and checked manually for fraud. The legitimate cases among these are issued Aadhaar number.*
- ***False Positive Identification Rate (FPIR): 0.057%**. In practical terms, it means that at a run rate of 10 lakh enrolments a day, only about 570 cases need to be manually reviewed daily to ensure that no resident is erroneously denied an Aadhaar number. The UIDAI currently has a manual adjudication team that reviews and resolves these cases. After manual adjudication, there is a negligible number of legitimate residents who are wrongly denied an Aadhaar number.*
- ***False Negative Identification Rate (FNIR): 0.035%**. This implies that 99.965% of all duplicates submitted to the biometric de-duplication system are correctly caught by the system as duplicates. Given that currently approximately 0.5% of enrolments are duplicate submissions, only a few*

thousand duplicate Aadhaars would possibly be issued when the entire country of 120 crores is enrolled.

The analysis resulting from such a large data set (8.4 crore records) is empirically repeatable and statistically accurate. There is no longer a need to rely on small sample size tests or hearsay from other projects. The UIDAI is now capable of measuring the accuracy, performance and scalability of the actual production system, which is already among the largest in the world. The results lay to rest unfounded claims that the underlying technology is untested, unreliable and based on unproven assumptions.

Based on the analysis, it can be stated with confidence that UIDAI enrollment system has proven to be reliable, accurate and scalable to meet the nation's need of providing unique Aadhaar numbers to the entire population. It is now safe to conclude that the system will be able to scale to handle the entire population

Abbreviations :

ABIS Automatic Biometric Identification System

API Application Programming Interface

CIDR Central Information Data Repository

FPIR False Positive Identification Rate

FNIR False Negative Identification Rate

FTE Failure to Enroll

NFIQ NIST Fingerprint Image Quality

POC Proof of Concept

SDK Software Development Kit

STQC Standardisation Testing and Quality Certification Directorate

UIDAI Unique Identification Authority of India

Contents

246

1 Introduction

247

UIDAI has adopted use of biometrics technology as part of its core strategy2in meeting its goal of preventing issuance of duplicate identity number to a resident. There is no method or technology, other than biometrics, that can catch a person who is disclaiming his real identity. Biometrics consists of methods for uniquely recognizing human beings based on one or more of their intrinsic physical or behavioural traits. By matching a person's biometric characteristics with everyone else's (known as de-duplication), the technology helps prevent issuance of duplicate identity (Aadhaar number) to a single person.

Identity documents that rely only on demographic fields and personal reference checks are surrogates of identity and are vulnerable to forgery, falsification, theft, loss, and other corruptions. In western countries such as the United States and the United Kingdom, documents such as driver's license, and passports are used as identity proofs but only because of the reliability of the birth certificates. A birth certificate acts as a breeder document (in conjunction with identity documents of the child's parents) in obtaining identity document for the child. Even in countries with reliable birth certificates, the issuance of identity documents in a way that assures a 'one person/one identity' policy has been problematic. This model does not work in India, so UIDAI's strategy has been to minimize dependence on unreliable breeder and identity documentation and to not depend upon the trustworthiness of the operator, but rather to leverage automation and technology in a way that reduces the total dependence on error-prone documents and people based processes.

2. Biometric Design Methodology

248

The UIDAI biometric system design has followed global best practices. In designing UIDAI's biometric system, UIDAI reviewed existing state-of-the-art biometric systems, consulted with the world's top biometric experts, conducted a proof of concept study and built a biometric system that is currently considered to be world's best and widely acknowledged to be so in numerous international biometric forums and conferences. UIDAI technical experts visited two of the world's largest biometric implementations: US-VISIT program and US Visa/Consular system. They had meetings with a large number of experts from several countries including Mexico, Bangladesh, UK, the US, Singapore and Australia. Two of the world's most renowned biometrics experts – Prof. Anil Jain3 and Prof. James Wayman worked with the UIDAI team and helped with the design. Prof. Anil Jain is pre-eminent biometric expert and advisor to many national and international governments. Prof. Wayman has served as an expert to numerous national ID system programs including UK, Philippines and the US. Several other biometric experts including Prof. Arun Ross4, Prof. John Daugman5 and Prof. Venu Govindaraju6also contributed to UIDAI's design.

UIDAI technical staff visited, reviewed and analyzed existing biometric programs in India including E-shakti NREGA scheme in Bihar, Coastal ID card of RGI, Orissa's UNWFR program. AP's Iris based ration card enrollment, Employees State Insurance Scheme of India (ESIC) and RSBY. These learnings were incorporated into a report published in December of 2009 by the UIDAI's Biometrics Standards Committee 7. Analysis of some of the programs is referenced in the committee's report. Based on other programs' results, the report acknowledged that fingerprint-

only system might present challenge in India due to majority of population being engaged in manual labour and advised that UIDAI to consider using iris to complement fingerprints in order to improve inclusiveness and accuracy of the system.

In December of 2010, The UIDAI published a Proof-of-Concept (PoC) study8 of biometric enrolments that were conducted between March 2010 and June 2010 in the predominantly rural areas of Andhra Pradesh, Karnataka, and Bihar. The UIDAI also carried out biometric enrolment of school children in the vicinity of Bangalore. About seventy five thousand people in all were enrolled during the first phase of the PoC study including people over 90 years of age,, and sixty thousand of the same people were re-enrolled during the second phase after a gap of three weeks, in order to test the biometric matching efficiency using known duplicates. While the biometrics committee report based its recommendations upon learnings from other programs and experts, the proof-of-concept study aided the UIDAI team in getting first hand field experience and in measuring the various process and accuracy parameters. It also confirmed empirically, the earlier recommendation of the 'Biometrics Standards Committee' that using iris in conjunction with fingerprints was a prudent decision.

The PoC was conducted to evaluate technical, operational, and behavioral hypotheses related to both the use of biometric devices and the overall enrolment process itself. It was also conducted to establish a baseline for the quality of biometric data that could be collected in rural India.

Figure: Fingerprint and Iris biometric

The key findings of the POC report, which have been presented internationally at scientific conferences and received extensive peer review, are listed here:

1. The PoC was successfully conducted over 1,35,000 biometric enrolments9. The relative ease of conducting the operation confirmed that biometric enrolment conforming to UID standards of quality and process was indeed possible on a large scale in rural India. The total biometric enrolment time for each individual, on average, was a little over three minutes. Of this, iris enrolment took a little under a minute, and was not perceived to be excessively difficult either by the resident or the enrolling operator. Specifically, many blind people also had their iris images captured successfully.

2. Multiple fingerprint scanners as well as iris capture devices were used in the PoC, and they performed according to expectations. The PoC was dispersed geographically and included many rural, often remote locations across three states. The enrolment was typically conducted with minimal infrastructure and sometimes in extreme weather conditions. Residents varied in age all the way from four years to about ninety years.

3. In general older people took longer to enroll than younger people, and residents whose employment involved manual work took longer to enroll than the rest of the PoC population. Older people needed more assistance from operators to capture their biometrics. However, the range of enrolment times observed was well within expectations implying that the enrolment exercise for the population was indeed practical.

4. The enrolment variations tested in the process led to the conclusion that the best process was one where the resident remained stationary during enrolment and the operator did the positioning of the devices.

5. The enrolment of children at the school showed that children in the age range of four to fifteen could be biometrically enrolled using the same process as that used for adults and with no additional difficulty. The match analysis also showed that their iris images and fingerprints could be de-duplicated as accurately as those of adults.

6. The quality of the biometric capture was sensitive to the setup of the enrolment station and the process itself. Most importantly, the enrolment operator's instructions made a significant difference in the efficiency of the biometric capture.

7. The quality check process built into the enrolment software was very important and provided helpful feedback to the operator in capturing high quality images. The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually. The multi-modal enrolment was adequate to carry out de-duplication on a much larger scale, with reasonable expectations of extending it to all residents of India.

The complete report is available on UIDAI's website. The final UIDAI design incorporated learnings from this PoC.

As of December of 2011, UIDAI has documented measurements taken from the real large-scale operational UIDAI system that has already issued over 10.25 crore (102.5 million) Aadhaar numbers. These measurements will be discussed later in this report under the heading of project status and system performance after we review the high level design of the UIDAI biometric system.

3. System Design

Following Biometric Standards Committee report, expert opinions, and learnings from the PoC, UIDAI selected three biometric modalities: face, all ten fingerprints and two irises. The decision to include iris in the UID initiative was a considered one, and took into account the critical needs of the project in ensuring the uniqueness of the Aadhaar number, and to also ensure that residents, particularly children and the elderly, are not excluded from enrolling for the UID. The PoC empirically demonstrated that iris is easy to capture, highly accurate, and not too expensive. By guaranteeing the universality and uniqueness of the UID, the initiative can have a substantial, transformational impact in the lives of residents.10

While the UIDAI Biometrics Standards Committee had already recommended the inclusion of iris, the PoC clearly demonstrated that iris capture was indeed necessary, and along with fingerprint, it was sufficient to de-duplicate and uniquely identify the entire population. The accuracy of the combined system is an order of magnitude better than fingerprints alone or iris alone, an important factor to consider for a population of 120 crore, and if the unique number is to be usable in high-security applications. Another reason for adding iris was inclusion. The use of iris also enables us to ensure the inclusion of the very poor, many of who work in physically intensive jobs, as well as children and the elderly. People working in jobs that require repeated use of fingers– for example, in fireworks factories or in areca nut plantations – often find their fingerprints degraded, which makes iris useful in ensuring uniqueness. The challenge with both fingerprint and face biometrics is that these have limitations when it comes to providing a unique number to children. Iris biometrics however, is reasonably stable in most persons, and can be collected from children as

young as five years of age. This is an important factor considering the multiple programs aimed at child welfare.

The enrollment system is designed in two major parts: i) client-side and ii) server-side. The client-side is responsible for operator-assisted collection of relevant data from the resident in the field. The data is collected by client software provided by UIDAI which immediately encrypts and applies a digital signature to the data so that no one other than UIDAI's server can decrypt it, not even the operator, enrolling agency or even the registrar. Since data is encrypted, UIDAI's multi-registrar approach improves scalability and provides choice to residents without any negative effects on the data security. The encrypted data is transmitted to UIDAI Central Information Data Repository (CIDR) where it is fed to the server-side system. The backend server-side system uses multiple automatic biometric identification systems (ABISs) to determine whether the resident is unique (that is, the resident has never received another Aadhaar number before). The Aadhaar letter containing the UID number (assuming that the server found the resident to be unique) is sent from the server-side system back to the resident through a letter delivered by the department of post.

3.1 Enrollment software: Client side

The client-side system is used by trained and *certified* enrollment operators in the field to collect relevant data from residents. The data collected includes demographic and biometric data. As long as the resident has met the requirements under one of document/introducer/NPR methods, the resident will not be denied enrollment. *Biometric failure to enroll is not a reason to deny enrollment in Aadhaar.* Key features of the client-side system are:

1. **Standardization.** UIDAI has standardized demographic data and biometric data formats. Client software is provided by UIDAI to achieve consistency across the nation. . NPR has also adopted the same standards for their enrollment.

2. **Open source and avoidance of vendor lock-in.** Client software is supported on both open source Linux and Microsoft Windows platforms. To promote competition and avoid vendor lock-in, UIDAI has standardized the Application Programming Interface (API) between the devices and client software to allow use of any certified device. A total of eleven different devices (five fingerprint devices and six iris devices) have been tested and certified by STQC.

3. **Quality.** Strong and sophisticated quality control measures and checks are built intricately into the client software. The operators of the system are required to go through rigorous training and certification process for high quality of data and consistency across the country.

4. **Security.** The data collected by the UIDAI client software is immediately encrypted and signed by the software such that it can only be decrypted by the UIDAI server. No other party can access data at source or in transit.

The client-side system, while geared towards enforcement of correct data collection process and policies, also includes a number of methods geared towards decreasing failure to capture and failure to enroll of biometric data and lowering the biometric de-duplication errors at the back-end. Few examples of checks and balances implemented at the client-side system are as follows:

1. Each biometric capture device is required to have a built-in auto-capture capability which ensures that biometric images are captured only when

deemed to be valid fingerprints slap or iris images and are of sufficient quality.

2. Biometric data quality is measured using standardized automated algorithms and thresholds are utilized to decide whether a captured sample is insufficient quality to warrant immediate re-capture.

3. The enrollment client performs a number of consistency checks. For instance, it makes sure that each biometric capture attempt comes from the same resident (instead of coming from operator, family member or previously enrolling resident).

4. The client software confirms that all 10 captured fingerprints are distinct as well as the two irises are distinct. It ensures that no repeated biometrics is captured.

5. The captured biometric is checked against that of the operator and the residents who enrolled previously on the same computer to avoid any chance of mix-ups.

6. Any biometric exceptions such as missing fingerprint or iris are logged and supervisor verification is required. In extreme cases such as missing both hands and/or missing both eyes, additional photograph of the hand and face is taken for proof of disability.

7. Operator overrides of the policies set in the software are logged to facilitate further investigation of the capture process and operator actions.

8. The images from all attempts (up to four) are included in the resident data packet and sent to server for processing.

3.2 Enrollment software: Server side

The server-side system is designed to scale to very high data and compute requirements as biometric de-duplication technology is computation and data intensive. Three main sub-systems on server side are utilized to provide highest accuracy while scaling to handle 120 crore population goal.

Duplicates are identified at each level. Different algorithms also ensure that false rejection of Aadhaar number does not occur at any level.

- Demographic de-duplication
- Multi-ABIS Multi-modal Biometric de-duplication (using multiple ABISs and multi-modal biometrics of 10 fingerprints and 2 irises)
- Manual adjudication (primarily to resolve records identified as duplicates found by previous stages)

Demographic de-duplication is used primarily to catch trivial duplicates(non-fraudulent cases where all the demographic fields are identical) that are inadvertently submitted to the system, for example when a resident has not received Aadhaar number in a few days and decides to re-enrol at an enrollment station again. Secondarily, it is also used for children under the age of 5 year as biometrics is not captured for children that young. The UIDAI uses both exact-match and fuzzy-match strategies to improve the demographic de-duplication accuracy.

Multi-ABIS Multi-modal Biometric de-duplication The biometric data de-duplication is at the heart of the system. The UID has procured 3 ABIS providers to perform biometric de-duplication, since they bring significant advantages:

1. The deployment of multiple ABISs improves the accuracy of de-duplication. If any ABIS identifies a potential duplicate, it is sent to the other ABIS for verification. By combining the results of all 3 ABIS's the overall biometric de-duplication accuracy goes up.
2. The utilization of three different de-duplication engines with different implementations and different fusion strategies also helps to detect various kinds of software or data collection errors. In certain enrolments (for

example in suspected duplicates and enrolments with poor quality biometrics) the enrollment data is sent to more than one ABIS to minimize the chance of an identification error. Another fascinating aspect of the continuous improvement process, originates from the feedback that is provided from the server-side system to the enrollment agency about the quality of their data. When enrollment agencies receive frequent report on the quality of their enrolments, it leads them to improve their training and processes – since their payments are linked to successful Aadhaars generated and not number of enrolments conducted. This improvement clearly shows up in measurements of quality that is performed frequently at the back-end.

3. The three ABISs compete for work based on their throughput capacity. This competition allows for continuous improvement in throughput and accuracy.

4. By distributing and sharing the de-duplication load across the 3 ABIS vendors the multi-ABIS solution gives the system a threefold increase in throughput. This is the reason why the UID system is able to achieve 10 lakh Aadhaars/day.

5. It ensures that the there is no vendor lock-in, if one of the ABIS vendors needs to be replaced (for whatever reason - technical or contractual) it can be done without bringing the entire system to a grinding halt.

Manual adjudication (required for duplicates found by the ABIS) is implemented as a semi-automatic process. The duplicates found by ABIS are processed by biometric SDKs to check if a process related issue has caused this (for example, mix of operator and resident biometric or repeated biometric of the resident etc.). Finally, the duplicate is analyzed

manually and the final decision is made by a human expert, leaving negligible chance that a legitimate resident is denied Aadhaar.

Security & Data Privacy: UIDAI system has been designed with utmost care to ensure security and privacy of data. Several features have been implemented to ensure that the resident's data remains completely private even within UIDAI partners and stakeholders, these are:

1. The data being sent to ABIS is completely anonymized meaning none of the ABIS systems have access to resident's demographic information (name, address, gender and date-of-birth), they are only sent biometric information of a resident with a reference-number and asked to de-duplicate. The de-duplication result that the ABIS returns with the reference number is mapped back to the correct enrolment-number by the UID's own enrolment server. This is akin to removing names from an examination answer paper so the examiner does not know whose paper he is evaluating.
2. The ABIS providers only provide their software and services. The data is stored in UID storage and it never leaves the UID's secure premises.
3. They ABIS providers also do not store the biometric images (source), they can only store template for the purpose of de-duplication.
4. The enrollment packet after it is encrypted by the enrolment client software in the field is sent to the UIDAI's CIDR (Central Identity Repository), the enrolment server decrypts the packet for de-duplication but never stores the decrypted packet in storage.
5. The original biometric images of fingerprints, irises and face are archived and stored offline and hence cannot be accessed through an online network.

4 Project Status & System Performance

259

There are over 36,000 active enrollment stations operated by 83 active enrollment agencies contracted through 59 active registrars across 32 states and union territories. Each station enrolls 50 residents per day, on an average. As many as eleven different models of fingerprint and iris devices are deployed in the field.

As of 31st December 2011, more than 15crore (150 million) enrolments have taken place in the field using UIDAI's client-side system, and over 10.25 crore (102.5 million) Aadhaar numbers have been generated by the server-side system. The overwhelming majority of the remaining nearly 5 crores is in transit from the field to the data center. The throughput has consistently increased since the start of the program both in the field and at the server back-end. In the month of December of 2011 alone, 2.23 crore (22.3 million) Aadhaar numbers were generated. The system is capable of processing at the rate of 10 lakhs (1 million) Aadhaar numbers per day and will continue to ramp up to meet the anticipated growth. The system is now the largest in the world based on its daily processing rate and one of three largest in terms of its database size. It is already the largest multi-modal biometric deployment in the world. The system produces daily measurements of - accuracy, throughput and quality. These measurements are based on industry wide accepted methods of calculating accuracy and quality. It should be emphasized that the system is now sufficiently large to clearly estimate the performance necessary to enrol the entire population. The system performance can no longer be a matter of speculation or extrapolation from small samples. It is unnecessary and inaccurate to attempt to infer UIDAI system performance from other systems which are ten to thousand times smaller.

Three key measures define the system effectiveness

260

1. **Biometric Failure to Enroll rate.** Per UIDAI policy, failure to enroll in Aadhaar is not allowed. That is, Aadhaar is a right of every Indian resident and cannot be denied. Therefore overall failure to enroll is set by policy to be *zero*. However, if certain residents are not able to provide their biometric (called B-FTE henceforth), biometric de-duplication cannot be carried out on their enrollment. Therefore the UIDAI measures B-FTE on an ongoing basis. It has been reported in a news item that this number in Indian context could be as high as 15%.

2. **False Rejection.** When new enrollment data from a resident is sent to CIDR, the system de-duplicates the resident packet to ensure that the resident has not previously been given a Aadhaar number. If the biometric de-duplication system rejects the new enrollment as being a duplicate, it is checked by manual adjudication process. If biometric system makes lots of errors, the volume of cases to adjudicate can go up significantly. This error by the biometric system is called false rejection of Aadhaar or False Positive Identification Rate (FPIR) of the biometric system. FPIR is a technical term and has very precise meaning in biometric literature. It has been reported in a news item that CIDR's FPIR could be so high to render the system useless.

3. **False Acceptance.** When new enrollment data from a resident is sent to CIDR, the system performs de-duplication to ensure that the resident has not previously been given an Aadhaar number. If in case the biometric system accepts the resident as new when in reality it was actually a duplicate, the resident will end up with two Aadhaar numbers. This error by the biometric system is called false acceptance of Aadhaar or False

Negative Identification Rate (FNIR). FNIR is a technical term and has very precise meaning in biometric literature.

4.1 Measured System Performance

It is now possible to carry out full scale performance measurement of real UIDAI production system and not rely on small samples or hearsay about other projects. The measurements were thus carried out on the entire database (called gallery) using large number of identification records11(called probes) when the UID database size reached 8.4 crore records.

1. **Failure to Enroll (B-FTE).** The biometric failure to enroll rate is measured to be 0.14%. **It means that 99.86% of the population has biometric that is usable for de-duplication purpose.** The exceptions (0.14%) of the population were not able to provide fingerprint and iris images and thus would be de-duplicated using demographic data and checked manually for fraud. The legitimate cases among these will be issued Aadhaar number. The UIDAI's actual B-FTE of 0.14% is more than 100 times lower than speculated in unfounded reports critical of the system.

2. **False Reject of Aadhaar (FPIR). FPIR is computed in the operational system by submitting a new record** to the system for de-duplication. If the system finds a duplicate (a HIT is said to have occurred), the pair is manually inspected and if the HIT is returned by the system in error, it is counted towards false positive identification errors. An **FPIR of 0.057%** was measured when the gallery size was 8.4 crore (84 million) and probe size was 40 lakhs (4 million). The false rejects (legitimate residents who are falsely rejected by the biometric system) were a count of 2309 out of the 40

lakh probes. These must go through adjudication process that involves manual review where the errors from the biometric system are corrected. In practical terms,it means that at a run rate 10 lakhs enrolments a day, only about 570 cases need to be manually reviewed daily to ensure that no resident is erroneously denied an Aadhaar number. Although this number is expected to grow as the database size increases, it is not expected to exceed manageable values even at full enrolment of 120 crores. The UIDAI currently has a manual adjudication team that reviews and resolves such cases.

3. **False accept (FNIR):** To compute FNIR, 31,399 known duplicates were used as probe against gallery of 8.4 crore (84M). The biometric system correctly caught 31,388 duplicates (in other words, it did not catch 11 duplicates). The computed FNIR rate is **0.0352%.** Assuming current 0.5% rate of duplicate submissions continues, there would only be a very small number of duplicate Aadhaars issued when the entire country of 120 crores is enrolled. Aadhaar expects to be able to increase the quality of all collections as the system matures. Consequently, we expect the potential number of false acceptances to decrease further below this already operationally satisfactory number.

4.2 Scaling to 120 Crore

Performance

As the UIDAI enrols more people, more resources are required to perform biometric de-duplication. The CIDR will require more computing resources as the data base grows. However, this process is extremely scalable (parallelizable) and throughput can be maintained with the addition of

hardware. UIDAI has done sufficient modeling as it grew from one crore to ten crore, it can be stated with high confidence that this throughput can be maintained till the entire nation is covered. In fact, the design of UIDAI system is such that throughput can be increased beyond 10 lakhs per day with reasonable addition of hardware.

Accuracy

Similarly, as the UIDAI enrol more residents, the internal parameters of the biometric system need to be adjusted to ensure that the biometric accuracy of the system does not degrade as the database grows.

Three well understood and accepted phenomena help us adjust these internal parameters.

1. False accept (FNIR) rate remains steady and does not increase with the increase in the database.
2. False reject (FPIR) rate grows linearly with the database size.
3. It is possible to trade off FNIR with FPIR. In other words, if we decrease FPIR, FNIR will increase. This relationship is modelled as "receiver operating characteristics (ROC)" and has very precise meaning in the biometric literature. UIDAI has modelled this relationship on the real production data.

Based on the model, the UIDAI expects the accuracy of the system to remain within the same order of magnitude as reported above. Hence it can be stated that system will be able to scale to handle the entire population without significant drop in accuracy.

5 Analysis

It is instructive to analyze the results to help us learn and make improvements in the system going forward.

5.1 Duplicates found correctly

In the previous section, when looking at results of FNIR, it was observed that a majority of duplicates found by the biometric de-duplication system are indeed found correctly. It is important to analyze these duplicates and understand why they are occurring. Some examples of duplicates being submitted to the system (and correctly caught by the system) are as follows:

1. Mixed biometrics: In this case, multiple attempts of the same modality (say fingerprints) belong to two different individuals. Among the duplicates, this issue was relatively frequent as it accounted for approximately 20% of the duplicates (correctly found by the ABISs). This issues is likely to have occurred due to operators not following due process. It has now been resolved with newer versions of the enrollment client software that includes checks to prevent this situation.
2. Anomalous biometrics: In this case, each modality is consistent, but different modalities have been captured from different individuals. Among the duplicates this issue was also relatively frequent as it accounted for approximately 20% of the duplicates (again, correctly found by the ABISs). Improvements in the enrollment client software will also reduce the incidence of such cases.

This analysis has resulted in UIDAI taking corrective action and building checks and balances in the enrollment client software so that the issue of inadvertent submission of duplicates can be eliminated in the field at the

client-side system. The advantage of addressing such issues at the client side is that the operator and resident are still present at the enrollment location and can take corrective action immediately.

5.2 Impact of biometric sample quality

It is well known from the biometrics scientific literature that quality of biometric samples play an important role in the accuracy of biometric matching. For this reason, it was deemed important to measure and control the quality of biometric data in both the client-side system and the server-side system. The client-side system has checks and balances (for example, automated capture that determines presence of good quality biometric, quality-based re-capture, etc.) that enforces capture of good quality data from the field. The server-side system aggregates the quality information and analyzes it with respect to different geographic regions, enrollment agencies, individual operators, biometric devices, etc.

At the time of writing of this report, the following measurements were obtained:

1. **Poor quality fingerprints**: 2.9% of residents were measured to have poor quality fingerprints as defined by their fingerprints yielding a score of 4 or 5 (on a scale of 1-5 with 5 being the worst quality) by the National Institute of Standards and Technology (NIST) NFIQ fingerprint image quality algorithm. By examining the records with low quality fingerprints, it is observed that majority of people who have poor quality fingerprints actually have good quality irises. It is important to note that for this group of people, the poor quality of their fingerprints alone does not degrade the de-duplication accuracy of the multi-modal biometric system.

2. **Poor quality fingerprint and poor quality irises:** 0.23% of residents have both poor quality fingerprint and poor quality irises. These are the residents who are susceptible to errors from the multi-modal biometric de-duplication system. Therefore, UIDAI team pays significant amount of effort in refining processes and building checks and balances in the system to measure, control, and reduce poor quality biometric data. It should be noted though that the state-of-the-art ABISs (such as those procured by UIDAI) are well versed in dealing with poor quality biometric data. Yet, by keenly measuring the quality and continuously improving the process that improves the quality of biometric data, UIDAI is making sure that the quality of collected biometric data stays high and does not degrade. This gives us the confidence that the system will scale to the entire population with the same quality of biometric as measured at the time of writing of this report.

6 Conclusion

In December 2009, UIDAI committee on biometrics published its report titled "Biometric Design Standards for UID Applications". The committee acknowledged that most other large-scale biometrics deployments were fingerprint-only and a fingerprint-based system may present challenge in India due to high manual labour practiced by majority of the population. The committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group analyzed fingerprint data collected from Delhi, UP, Bihar, and Orissa and found that the quality of the data was actually not substantially different from the western population. The committee said that it is possible to improve the accuracy of fingerprint system especially considering the need to scale to 120 crore population by additionally using iris. "*Iris can provide*

accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy."12

In December of 2010, UIDAI published a report titled "UID Enrollment Proof-of-Concept Report". The report documents the findings of enrollment proof-of-concept study commissioned by UIDAI in three rural areas of Andhra Pradesh, Karnataka, and Bihar. Among many interesting findings on both process and technology, the report says "*The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually. The multi-modal enrolment was adequate to carry out de-duplication on a much larger scale, with reasonable expectations of extending it to all residents of India*". 13.

As of December 2011, the UIDAI has true and tested statistics computed from real operational large-scale UIDAI system at a gallery size of 8.4 crore (84 million), which is more than 4,000 times the sample size that was available at the time of enrollment PoC. There is no longer a need to rely on small sample size tests or hearsay from other projects. The UIDAI is now capable of measuring the accuracy, performance and scalability of the actual production system, which is already among the largest in the world. The analysis resulting from such a large data set is empirically repeatable and statistically accurate. Based on the analysis, it can be said that the enrollment system has proven to be reliable, accurate and scalable to meet the nation's need of providing unique Aadhaar numbers to the entire population. Specifically, the following are observed:

1. **Failure to Enroll(FTE) Rate**: Zero. As a policy, every unique resident, regardless of their biometrics can be enrolled and issued Aadhaar number. 268

2. **Biometric Failure to Enrol (B-FTE) Rate: 0.14%.** This implies that 99.86% of the population can be uniquely identified by the biometric system. The exceptions (0.14%) however can still be de-duplicated using demographic data and checked manually for fraud. The legitimate cases among these will be issued Aadhaar number.

3. **False Positive Identification Rate (FPIR): 0.057%.** In practical terms, it means that at a run rate of 10 lakh enrolments a day, only about 570 cases need to be manually reviewed daily to ensure that no resident is erroneously denied an Aadhaar number. Although this number is expected to grow as the database size increases, it is not expected to exceed manageable values even at full enrolment of 120 crores. The UIDAI currently have a manual adjudication team that reviews and resolves such cases.

4. **False Negative Identification Rate (FNIR): 0.035%.** This implies that 99.965% of all duplicates submitted to the biometric de-duplication system are correctly caught by the system as duplicates. Given that currently approximately 0.5% of enrolments are duplicate submissions, there would only be a very small number of duplicate Aadhaars issued when the entire country of 120 crores is enrolled.

5. **Scalability.** The system is currently processing 10 lakhs (1 million) enrolments a day with enrolment database (gallery) of 9.8 crore (98 million). It has scaled (grown) as expected. The additional computing power required to handle increasing number of enrolments will not grow at an

abnormally high (non-linear) rate; it is well within the design and expectations of the UIDAI.

The key measures reported above have also been computed at different gallery sizes up to 8.4 crores. Based on the trend, the UIDAI expects the accuracy of the system to remain within the same order of magnitude as reported above. It is now safe to conclude that the system will be able to scale to handle the entire population. The results lay to rest unfounded claims that the underlying technology is untested, unreliable and based on unproven assumptions.

It is the policy of Aadhaar to maintain continuous quality improvement. Consequently, UIDAI will continue to monitor performance, adjust parameters as needed and institute new processes and procedures to not only maintain the currently low error rates, but to even improve system performance as the system grows to the ultimate goal of 120 crore.